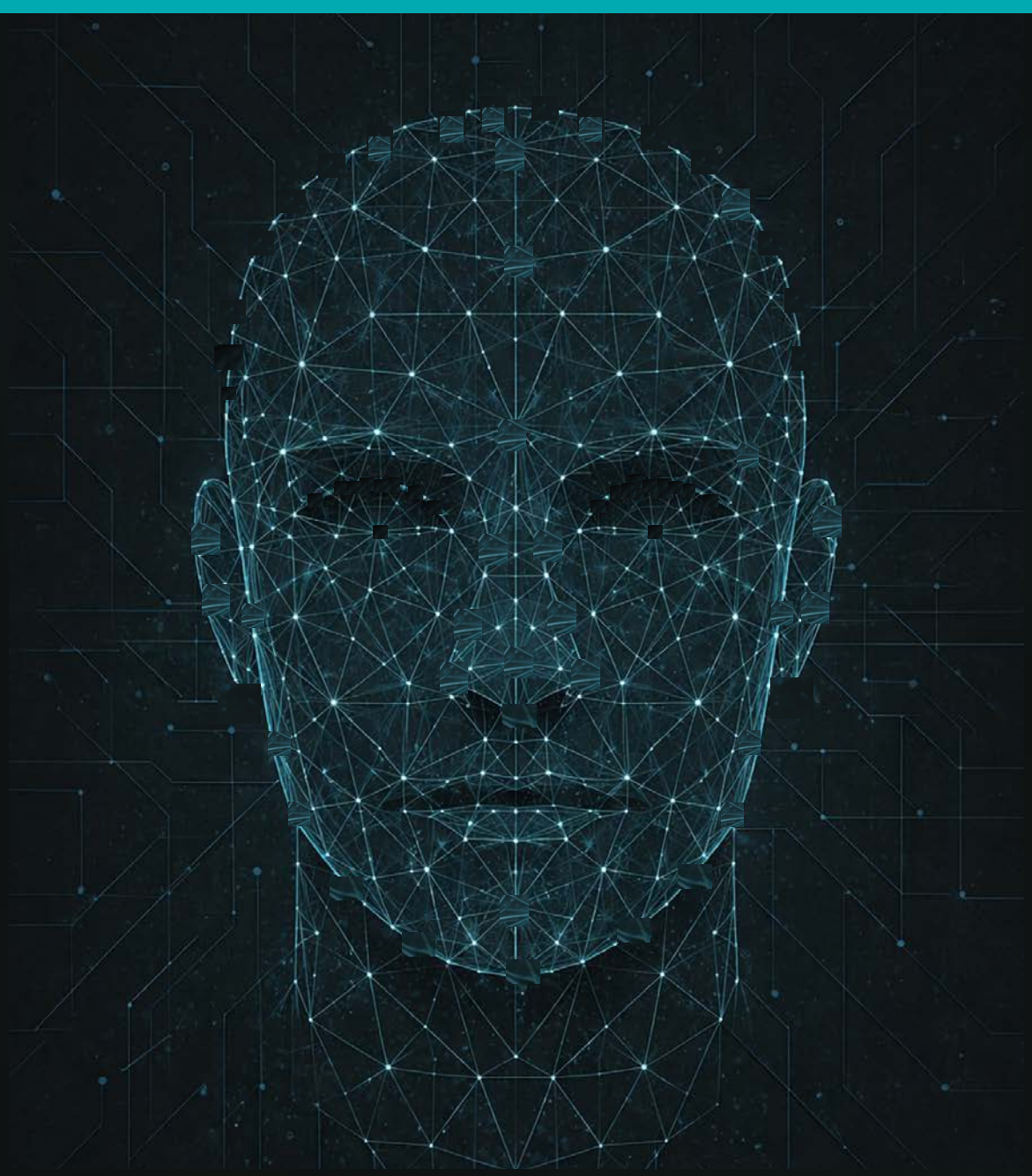
Ribas
Artículos
Publicaciones
Versión 1.0 - 08/01/2026

En 2025 se produjeron ligeros avances en materia de datos biométricos que parecen indicar un tratamiento jurídico cada vez más razonable.

Los datos biométricos después de AENA

Ligeros avances hacia un enfoque más moderado



ribas

Ligeros avances

En 2025 se produjeron ligeros avances en materia de datos biométricos que parecen indicar un tratamiento jurídico cada vez más razonable y moderado.

También quedaron claros los requisitos para realizar un tratamiento ajustado al entorno regulatorio y a los criterios de las autoridades de control.

En este documento analizamos los avances y la lista de requisitos.

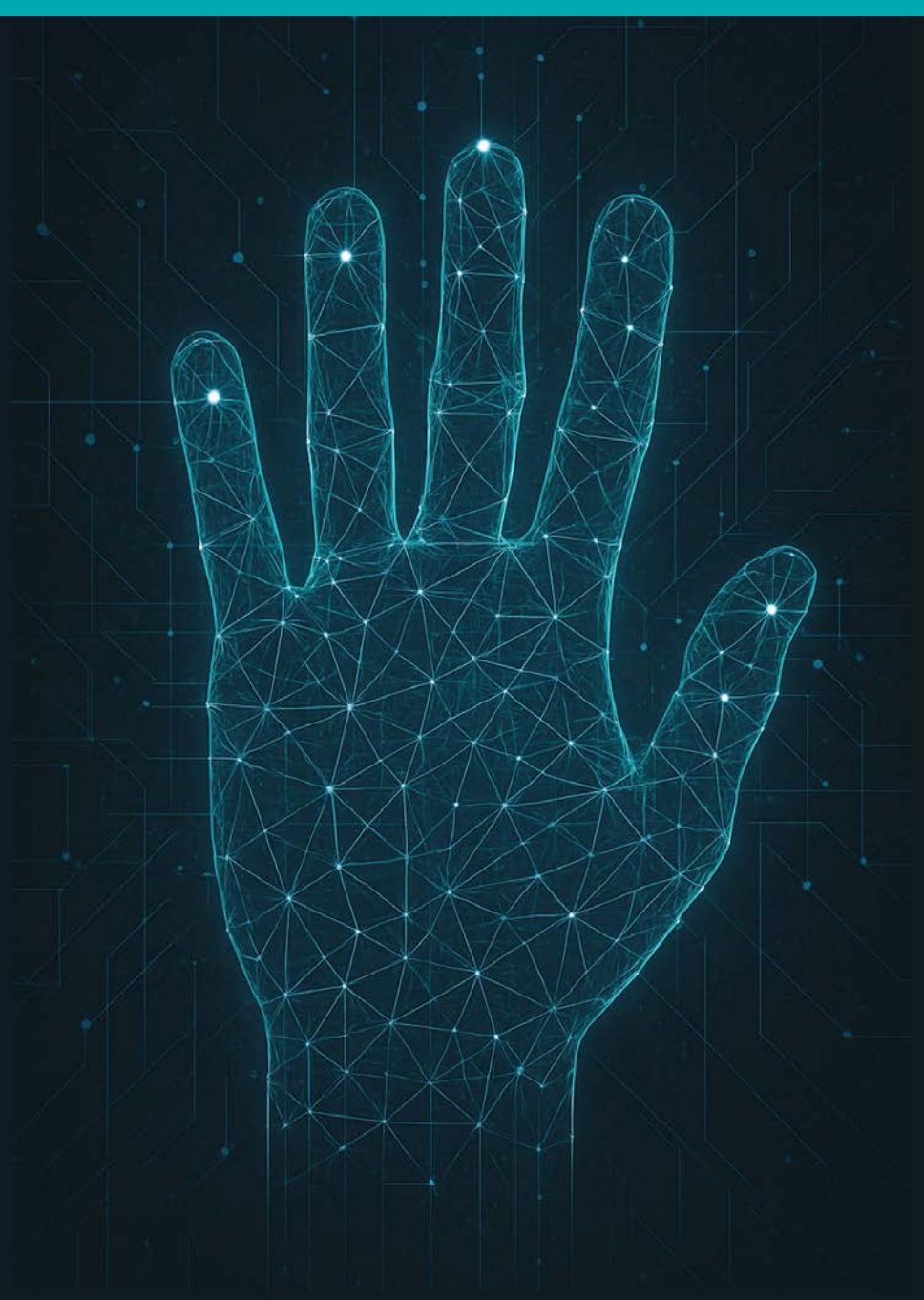
Abreviaturas

Abreviatura	Significado
CCN	Centro Criptológico Nacional adscrito al CNI y al Ministerio de Defensa
ENS	Esquema Nacional de Seguridad
RIA	Reglamento de inteligencia arttificial

Contenido del documento

Claves de la resolución de la AEPD

Cuestiones importantes de la resolución de la AEPD en el caso de AENA, en la que se aprecian avances en relación con la posición de anteriores resoluciones.



ribas

Almacenamiento y control del interesado

Se confirma la relevancia del almacenamiento de los datos biométricos en la valoración del control ejercido sobre los mismos, de acuerdo con los criterios del Comité Europeo de Protección de Datos manifestados en el Dictamen 11/2024. Los siguientes escenarios se consideran compatibles con el artículo 5 del RGPD.

Escenario 1. - Almacenar una plantilla biométrica registrada en manos de la persona, por ejemplo, en su dispositivo individual, bajo su control exclusivo, con el fin de autenticar (comparación 1:1) al interesado.

Escenario 2. - Almacenar de forma centralizada una plantilla biométrica registrada de forma cifrada con una clave o código secreto únicamente en manos del interesado y con el fin de realizar una autenticación mediante comparación 1:1.

PROPUESTA DIGITAL OMNIBUS

La iniciativa Digital Omnibus de la Comisión Europea contiene una propuesta de modificación del artículo 9.2 del RGPD, mediante la que se introduciría una nueva excepción a la prohibición del artículo 9.1, que sería aplicable en el caso de que el tratamiento de datos biométricos fuese necesario para la finalidad de confirmar la identidad del interesado (verificación), cuando los datos biométricos o los medios necesarios para la verificación están bajo el control exclusivo del propio interesado.

Tipo de control biométrico

Se confirma que la identificación genera más riesgo para el interesado que la autenticación.

El riesgo de un control biométrico basado en una comparación uno-a-varios (1:n) es superior que el generado en una comparación uno-a-uno (1:1)

En la resolución de AENA la AEPD indica que el control biométrico se realiza empleando un sistema de identificación que implica una operación uno-a-varios (1:N), que desde el punto de vista de protección de datos implica una búsqueda activa dentro de un conjunto de identidades preexistentes, lo cual puede comportar mayores riesgos para los derechos fundamentales de las personas físicas.

La AEPD considera que no todos los tratamientos de categorías especiales de datos comportan el mismo nivel de riesgo ni exigen el mismo grado de salvaguardas. Desde una perspectiva de la legalidad y, especialmente de la proporcionalidad y evaluación de riesgos, la identificación (1:N) suele presentar mayores riesgos para los derechos y libertades fundamentales, en especial por su carácter invasivo.

La Agencia añade que dentro de los métodos que utilizan datos biométricos, los basados en reconocimiento facial pueden ser incluso más intrusivos que otros, como los de detección de huella dactilar.

Finalidades

Se confirma que es un gran error tratar las finalidades en bloque.

El procedimiento recomendado es el siguiente:

1. Identificar todas las finalidades del tratamiento.
2. Clasificar las finalidades por grupos.
3. Agrupar las finalidades que generan un beneficio directo para el responsable del tratamiento.
4. Agrupar las finalidades que generan un beneficio para el interesado o para la comunidad.
5. Diferenciar claramente las finalidades de cada fase del ciclo de vida del dato.
6. Incluir las finalidades en el gráfico o en la tabla descriptiva de cada fase del ciclo de vida.
7. Identificar claramente las finalidades instrumentales, es decir, aquéllas que están asociadas a los medios y a las herramientas seleccionadas para cumplir las finalidades últimas y esenciales del tratamiento.
8. Identificar claramente las finalidades últimas y esenciales del tratamiento.

Juicio de idoneidad

En la resolución de AENA la AEPD considera que el tratamiento llevado a cabo era idóneo para cumplir con la finalidad pretendida, que era la identificación unívoca de los pasajeros con derecho de acceso, tránsito y embarque.

La AEPD no es contraria a que AENA trate datos biométricos como método de control de acceso a determinadas zonas del aeropuerto, siempre y cuando:

1. El tratamiento se realice con las debidas garantías.
2. Tras el completo cumplimiento de los requisitos que impone el RGPD.
3. Entre ellos, llevar a cabo una EIPD en los términos del art. 35 del RGPD.
4. Que incluya un análisis sistemático de la necesidad y proporcionalidad de las operaciones de tratamiento que se pretenden realizar.

La AEPD no niega que el hecho de que no tener que mostrar la documentación para pasar los diferentes filtros de acceso hasta el avión vaya a resultar más cómodo para los pasajeros, así como que vaya a reducir tiempos y aglomeraciones, siendo estos beneficios para la entidad y los propios pasajeros. Estas ventajas o beneficios deberán considerarse en el posterior análisis de riesgo-beneficio que debe incluirse al valorar la proporcionalidad en sentido estricto, junto con el resto de las ventajas y desventajas concurrentes. Pero estas ventajas no determinan por sí solas que el sistema sea idóneo desde el punto de vista del tratamiento de protección de datos personales.

Se indicaba expresamente que: “podemos considerar inicialmente que el sistema de reconocimiento facial desarrollado por AENA podría superar el requisito de idoneidad para cumplir la finalidad real del tratamiento. Toda vez que el apartado 7 de la EIPD de AENA ofrece datos objetivos y contrastados de que los sistemas de reconocimiento facial podrían ser eficaces para servir como método eficaz de verificación de identidad (identificación unívoca fiable) de los pasajeros al objeto de permitir su acceso a las zonas aeroportuarias que se señalan en el proyecto, siempre que se configure con las medidas y garantías adecuadas”

Juicio de necesidad

Una vez confirmada la conveniencia de separar las finalidades y realizar un análisis independiente para cada una de ellas, las acciones recomendadas son las siguientes:

1. Verificar que el tratamiento es necesario para la finalidad pretendida.

2. En el caso de existir varias finalidades, verificar que el juicio de necesidad no está relacionado con todas las finalidades en bloque.

3. Verificar que el juicio de necesidad está relacionado con cada finalidad y con cada fase del tratamiento.

4. Valorar el nivel de afectación real de los derechos fundamentales del interesado.

La AEPD invoca la doctrina del Tribunal Constitucional y defiende que la limitación de los derechos fundamentales tiene que ser la indispensable y estrictamente necesaria para satisfacer el fin que se persigue, de manera que, si existen otras posibilidades de satisfacer dicho fin menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes.

La AEPD añade que la necesidad no debe confundirse con utilidad del sistema. Puede que el sistema de reconocimiento facial implantado por AENA facilite el no tener que llevar una tarjeta de embarque ni tener que mostrar el documento de identidad, que se tarde menos en su acceso, que sea automático e instantáneo y no excesivamente costoso. Y también que, como AENA señalaba en el juicio de idoneidad, pueda reducir riesgos de extravío o robo de documentos.

AENA indica que si se acepta la tesis de la Agencia, cualquier tratamiento que implique identificación biométrica sería considerado innecesario frente a la alternativa de verificación humana y que este criterio restrictivo de la Agencia contradice las posiciones adoptadas por otras autoridades de control y por el propio Comité Europeo de Protección de Datos (EDPB) en cuyo Dictamen 11/2024 del EDPB, relativo al uso del reconocimiento facial para agilizar el flujo de pasajeros en aeropuertos, analiza expresamente la compatibilidad de estos sistemas con el principio de minimización de datos del artículo 5.1 c) del RGPD.

Análisis de la viabilidad de alternativas

El análisis de la viabilidad de las alternativas es un elemento esencial del juicio de necesidad, por lo que las acciones recomendadas son las siguientes:

1. Verificar que se ha realizado un análisis de viabilidad de todas las alternativas conocidas y disponibles, incluidas las de la misma naturaleza con la misma idoneidad y eficacia.

2. Verificar si existen alternativas previstas en una norma con rango de ley.

3. Verificar si se ha documentado en la EIPD el estudio de viabilidad de las otras alternativas, indicando las conclusiones.

4. Verificar si se han obtenido evidencias objetivas que justifiquen que las alternativas menos intrusivas valoradas son menos eficaces o menos seguras.

5. Verificar que las evidencias contienen datos objetivos.

Juicio de proporcionalidad

Las acciones recomendadas en relación con el juicio de proporcionalidad son las siguientes:

1. Realizar el análisis del balance riesgo - beneficio.

2. Verificar que el análisis incluye todos los riesgos, beneficios, ventajas y desventajas.

3. Verificar que existe simetría entre la lista de beneficios y la lista de riesgos.

4. Verificar que el análisis se realiza desde el punto de vista de la protección de datos y no desde el cumplimiento de criterios de negocio, de eficacia o de eficiencia.

5. En el caso de existir varias finalidades, verificar que el juicio de proporcionalidad no está relacionado con todas las finalidades en bloque.

6. Verificar que el juicio de proporcionalidad está relacionado con cada finalidad y con cada fase del tratamiento.

7. Verificar que se ha realizado una ponderación de las ventajas y desventajas frente a las otras alternativas menos intrusivas.

Evaluación de impacto aplicada al ciclo de vida de los datos

Fase 1	Fase 2
Descripción de las operaciones a realizar	Descripción de las operaciones a realizar
Tabla de finalidades instrumentales	Tabla de finalidades últimas o esenciales
Beneficios para el RT y para el interesado	Beneficios para el RT y para el interesado
Análisis de riesgos inherentes	Análisis de riesgos inherentes
Tabla de riesgo - beneficio	Tabla de riesgo - beneficio
Base jurídica de cada finalidad	Base jurídica de cada finalidad
Excepciones del artículo 9.2 del RGPD	Excepciones del artículo 9.2 del RGPD
Juicio de idoneidad para cada finalidad	Juicio de idoneidad para cada finalidad
Juicio de necesidad para cada finalidad	Juicio de necesidad para cada finalidad
Juicio de proporcionalidad para cada finalidad	Juicio de proporcionalidad para cada finalidad
Medidas técnicas y organizativas a aplicar	Medidas técnicas y organizativas a aplicar
Cálculo del riesgo residual	Cálculo del riesgo residual
Conclusión final sobre el riesgo residual global y la viabilidad del tratamiento	

Análisis más amplio de la resolución de la AEPD

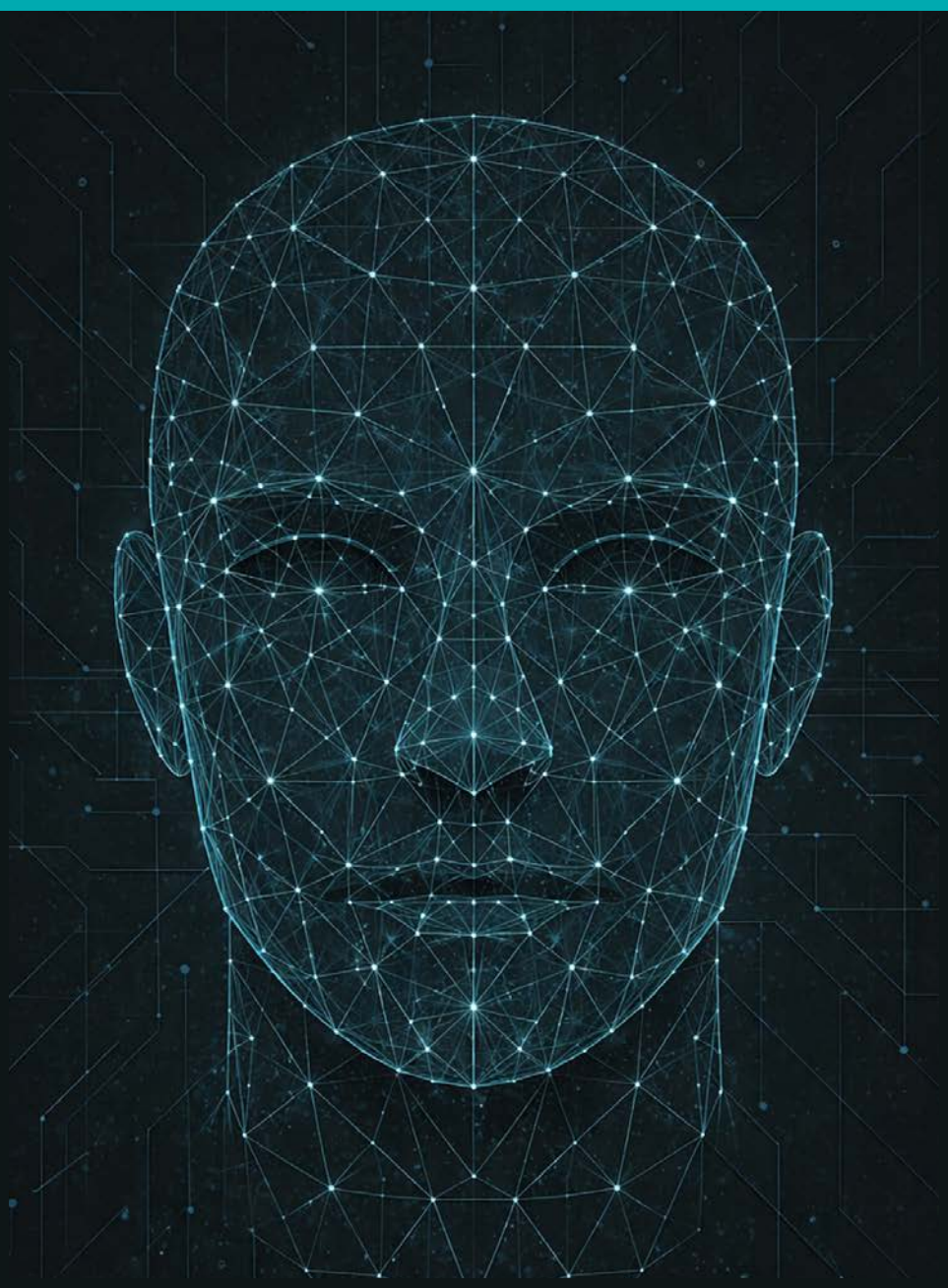
En este documento se analiza con mayor amplitud la resolución de la AEPD desde la óptica de los requisitos de una evaluación de impacto.

https://lnkd.in/e4CUf4Cy

ribas

Claves de la consulta previa de la Guardia Civil

Cuestiones importantes de la consulta previa formulada por la Guardia Civil a la AEPD en materia de control de acceso con datos biométricos.



ribas

Finalidad del tratamiento

La finalidad del tratamiento principal (COSEIN-ACCESOS) es la "identificación y control de personas ajenas, residentes, vehículos que acceden o autorizados a estacionar en el interior. Gestión sistemas acceso con identificación mediante tarjetas, biometría, u otro tipo que suponga tratamiento de datos personales."

El proceso de control previsto en la consulta previa no se trata de un nuevo tratamiento y la novedad radicaría, exclusivamente, en la implementación de un sistema de biometría para automatizar el acceso de las personas a las zonas y el tiempo definidos en la autorización previa.

Base jurídica

En el inventario de tratamientos COSEIN-ACCESOS, se señala que la base legal es el cumplimiento de una obligación legal; artículo 6.1.c del RGPD. Y el consentimiento del interesado; artículo 6.1.a del RGPD.

En la consulta previa se valora la aplicación de las siguientes normas:

1. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
2. Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.
3. Ley 9/1968 sobre secretos oficiales.
4. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
5. Real Decreto 179/2005, de 18 de febrero, que establece normas específicas sobre la prevención de riesgos laborales en la Guardia Civil, que implica que se debe asegurar la protección de sus instalaciones y del personal que opera en ellas y que, en la práctica, se traduce en la implementación de medidas de seguridad y protocolos de actuación para la vigilancia de sus propias instalaciones al objeto de garantizar la integridad del personal y la correcta ejecución de sus funciones.
6. Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.

No se considera aplicable la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, ya que se exceptúan de su aplicación las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.

Futura base jurídica

El anteproyecto de transposición de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas, incorpora una disposición adicional séptima que lleva por título el de “instalación de sistemas de reconocimiento biométrico”, que permite el uso de sistemas biométricos de la siguiente manera:

“En virtud de lo dispuesto en el artículo 26 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y teniendo en cuenta la Evaluación Nacional de Amenazas y Riesgos, las entidades críticas establecerán sistemas de reconocimiento biométrico de identificación o autenticación en todas o algunas de sus instalaciones con objeto de garantizar el control de accesos y el desplazamiento con fines de prevención de delitos y seguridad física. La implantación de estos sistemas, las características que deben reunir y su extensión, se regularán mediante orden del Ministro del Interior”.

Menor riesgo de la autenticación

No todos los tratamientos basados en el artículo 9 del RGPD comportan el mismo nivel de riesgo ni exigen el mismo grado de salvaguardas.

La distinción entre identificación o autenticación y especialmente de los elementos concretos de estos tratamientos tanto por sus fines como especialmente por los medios son elementos esenciales para determinar:

1. La proporcionalidad del tratamiento.
2. La necesidad de realizar una evaluación de impacto.
3. La graduación en la intensidad de las garantías a aplicar.
4. Los requisitos para el levantamiento de la prohibición del artículo 9.1 del RGPD.
5. La aplicabilidad de excepciones al tratamiento de datos biométricos, especialmente en ámbitos como el laboral, la seguridad pública o la prestación de servicios digitales.

La autenticación biométrica localizada, bien diseñada y según toda una serie de circunstancias a tener en cuenta en cada caso concreto, puede ser en muchos contextos más proporcionada y menos intrusiva, especialmente si existe regulación o consentimiento libre e informado y garantías adecuadas.

El principio de legalidad impone no sólo una base jurídica en abstracto, sino un grado suficiente de precisión y previsibilidad en función del riesgo y del impacto del tratamiento. No puede exigirse el mismo nivel de densidad normativa para una identificación masiva y automatizada sin conocimiento del afectado que para una autenticación puntual, consentida y localizada.

Regulación diferenciada de la autenticación

La Directiva (UE) 2024/2831 sobre trabajadores de plataformas digitales prohíbe expresamente el uso de datos biométricos con fines de identificación (1:N), es decir, mediante el cotejo de los datos de una persona con los de una base de datos de múltiples individuos. En cambio, permite la autenticación o verificación unívoca (1:1) con las garantías correspondiente a los datos especialmente protegidos cuando esta se limita a cotejar los datos del interesado con los que él mismo proporcionó previamente, siempre que el tratamiento sea lícito conforme al RGPD u otras normas aplicables (Considerando 41).

Reglamento (UE) 2024/1684 sobre inteligencia artificial, mantiene esa distinción operativa y jurídica (considerandos 14 y ss.). En particular, el Anexo III. 1º distingue claramente entre identificación biométrica remota (varios-a-varios, M:N), considerada de alto riesgo, y verificación biométrica (uno-a-uno, 1:1), que queda expresamente excluida cuando su única finalidad es confirmar la identidad declarada por una persona.

Puntos a tener en cuenta en la evaluación del riesgo

El impacto real sobre los derechos y la intensidad de las medidas de protección requeridas pueden variar sustancialmente, debiendo valorarse caso por caso en función de los siguientes elementos:

1. Contexto.
2. Escala.
3. Tecnología utilizada.
4. Control efectivo que conserve el interesado sobre sus datos biométricos.

.

Garantías recomendadas

En el caso de existir una regulación concreta del tratamiento de los datos biométricos, las garantías posibles que convendría incorporar podrían ser las siguientes:

1. Registro biométrico asistido por personal cualificado.
2. Exclusión de procesos desasistidos o delegados en terceros.
3. Datos biométricos bajo el control exclusivo del interesado.
4. Prevención de acceso o tratamiento por terceros.
5. Protección frente al fraude o la suplantación de identidad.
6. Prohibición del almacenamiento centralizado de identificadores biométricos.
7. Generación como tratamiento local, en sistemas aislados, sin conexión a redes
8. Imposibilidad de interoperabilidad con otros sistemas.
9. Revocabilidad de los identificadores.
10. Fecha de caducidad que limite su uso al tiempo estrictamente necesario.
11. Información clara sobre alternativas disponibles, riesgos del tratamiento, derechos del interesado y procedimientos de destrucción de los datos.
12. Conservación de los datos personales no biométricos durante 30 días, con bloqueo posterior.
13. Limitación del almacenamiento de información en los sistemas al tiempo necesario para cada autenticación, sin permitir su transmisión o conservación indebida.
14. Instalación de la infraestructura biométrica en ubicaciones controladas dentro de las propias dependencias de seguridad, en condiciones que garanticen la privacidad y la seguridad técnica.
15. Evaluación de impacto en la protección de datos.
16. Actualizaciones periódicas de la EIPD al menos cada cuatro años o cuando se produzcan incidentes relevantes o modificaciones sustanciales del tratamiento.
17. Cumplimiento del nivel alto del Esquema Nacional de Seguridad.
18. Auditorías periódicas.

Idoneidad

El tratamiento sería idóneo (esto es, serviría para) la finalidad pretendida, que es garantizar el control de accesos para conferir una intensa seguridad, que es la necesaria para el acceso a las concretas instalaciones.

El sistema de identificación biométrica está diseñado para ser apropiado al fin perseguido, ya que el tratamiento biométrico permite verificar con mayor fiabilidad que otros mecanismos quién accede a los espacios protegidos, evita suplantaciones de identidad y permite restringir accesos no autorizados.

Necesidad

En el ámbito técnico, existen desarrollos recientes en tecnologías biométricas que permiten reducir significativamente el impacto sobre los derechos de los interesados, especialmente cuando se aplican condiciones como la generación local de identificadores, la no interoperabilidad, la ausencia de almacenamiento centralizado, la imposibilidad de reversión y el control exclusivo por parte del propio interesado. Estas características, recogidas en el sistema analizado, reflejan una evolución hacia esquemas de autenticación biométrica más seguros y menos intrusivos, que pueden considerarse buenas prácticas en el diseño de sistemas de control de accesos con menor impacto.

En este sentido, el sistema implantado incorpora un conjunto relevante de garantías técnicas orientadas a la minimización del impacto, con medidas como la generación local de identificadores no reversibles, su validez limitada a los períodos autorizados, el control exclusivo del interesado sobre sus datos y su no interoperabilidad. El diseño, además, limita el reconocimiento a la persona situada directamente frente a la cámara, reduciendo el riesgo de tratamientos accidentales o masivos. Estas configuraciones permiten restringir el alcance del tratamiento y previenen usos indebidos o accesos no autorizados.

Estas medidas muestran una respuesta específica y proporcional al riesgo, frente a otras medidas muy posiblemente menos eficaces, como el uso de tarjetas, contraseñas o registros manuales, que podrían ser susceptibles de pérdida, cesión o manipulación. La biometría utilizada, aplicada con este diseño específico, incrementa la eficacia del control de accesos sin recurrir a almacenamiento centralizado y con estricta vinculación entre identificador y persona autorizada. En este caso, sin embargo, las medidas alternativas —como tarjetas físicas, PINs o control presencial— puede considerarse que no ofrecerían el mismo nivel de eficacia ni garantía frente a suplantaciones, accesos indebidos o vulneraciones de seguridad, especialmente en contextos con instalaciones sensibles. Por tanto, no procede exigir su sustitución por medidas menos intrusivas si estas no alcanzaran un grado de eficacia equivalente.

Proporcionalidad

En relación con la proporcionalidad en sentido estricto, que implica valorar si los perjuicios causados por la medida son desproporcionados respecto al objetivo perseguido, el sistema en cuestión incorpora numerosas garantías técnicas y organizativas que minimizan el impacto sobre los derechos de los interesados. La no centralización del almacenamiento, la caducidad de los identificadores, la imposibilidad de reversión, la exclusividad en el uso por parte del propio interesado y el aislamiento de los terminales, evidencian un diseño que busca mitigar riesgos desde su concepción.

Estas características descritas técnicamente en la documentación aportada refuerzan la evaluación positiva del sistema desde la perspectiva de proporcionalidad y minimización. Además, se plantea que en casos particulares (…) pueda evaluarse con mayor detalle la proporcionalidad en la EIPD, incluso valorando alternativas si resultaran igualmente eficaces y factibles. Esta
previsión evita soluciones uniformes allí donde el impacto pudiera ser mayor.

Puede concluirse que el tratamiento biométrico previsto en este sistema superaría en términos genéricos para este caso adecuadamente el juicio de proporcionalidad. La existencia de un diseño orientado a la minimización de riesgos, unido a la posibilidad de modulación en determinados contextos, asegura que este tratamiento no incurre en los defectos lógicos identificados en otros enfoques que confunden necesidad con menor intrusión o que omiten el análisis técnico de idoneidad.

ribas

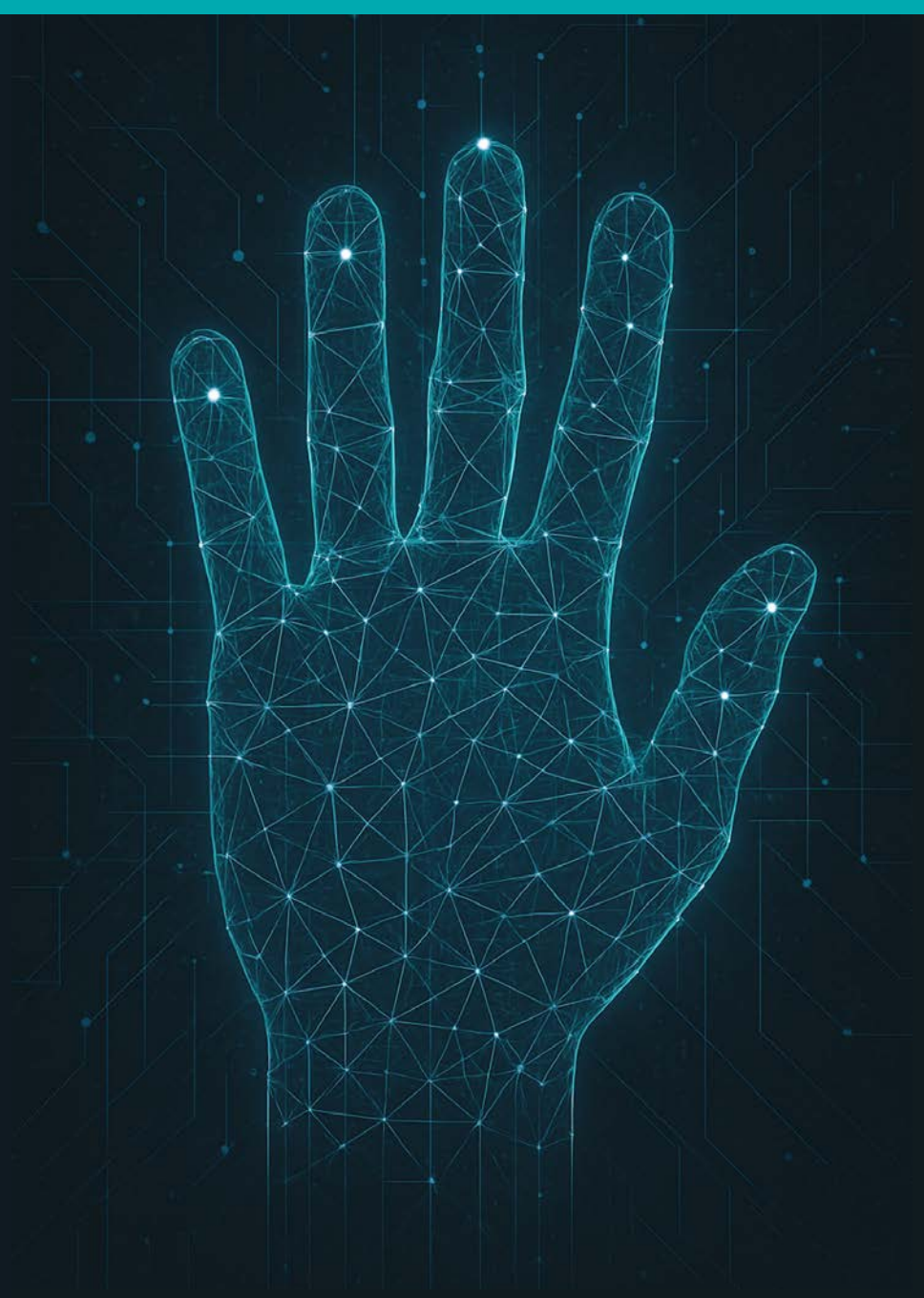
Conclusiones

1. Las medidas adoptadas en el tratamiento mitigan los riesgos suficientemente.
2. El tratamiento biométrico proyectado cuenta con la base legal y regulación suficiente.
3. El tratamiento cumple con los requisitos que exige el principio de proporcionalidad según la jurisprudencia del Tribunal Constitucional y el Tribunal de Justicia de la Unión Europea, al responder a un objetivo legítimo —la protección de instalaciones sensibles y la gestión de accesos en el ámbito de las competencias legalmente atribuidas a la Guardia Civil— y resultar adecuado para alcanzarlo.
4. Las medidas técnicas adoptadas, como la generación local de identificadores no interoperables ni reversibles, su control exclusivo por el interesado, la ausencia de almacenamiento centralizado y la limitación estricta a los fines de autenticación, garantizan la idoneidad de la medida frente a otras opciones menos eficaces.
5. La evaluación demuestra en términos razonables que no existe una alternativa igualmente eficaz que permita alcanzar los mismos fines con menor impacto.
6. En cuanto al requisito de las garantías aplicadas —junto con la posibilidad de ajustes en espacios residenciales o de menor criticidad— permiten afirmar que los perjuicios para los derechos de los interesados no resultan desproporcionados en relación con los fines perseguidos.

ribas

Miedo infundado a la suplantación de identidad con datos robados

No se ha encontrado una constancia documental, judicial ni técnica de un caso de suplantación de identidad ejecutado con éxito mediante la reutilización de plantillas biométricas robadas a un responsable del tratamiento.



ribas

Conclusión avanzada de este apartado

La conclusión avanzada de este apartado es que, a día de hoy, **no se ha encontrado una constancia documental, judicial ni técnica** de un caso de suplantación de identidad ejecutado con éxito mediante la reutilización de plantillas biométricas robadas a un responsable del tratamiento.

ribas

Brechas de datos biométricos más importantes

En esta tabla pueden verse los incidentes de seguridad más graves con afectación de datos biométricos y el contraste del carácter masivo del incidente con la ausencia total de quejas y denuncias por explotación de los datos y suplantación de identidad.

Las autoridades de control consideran la ausencia de quejas y denuncias como un indicador importante en la decisión de archivar la investigación de una brecha de seguridad, incluso en el caso de que los datos hayan sido publicados.

Caso	Datos comprometidos	Quejas o denuncias por suplantación de identidad
OPM (EE.UU., 2015)	5,6 millones de huellas dactilares	No constan
Biostar 2 (2019)	27,8 millones de patrones biométricos dactilares y faciales	No constan
Aadhaar (India, 2023-24)	815 millones de huellas dactilares	No constan Hubo fraudes cometidos con huellas clonadas de otros registros públicos, pero no directamente de este incidente.
Oracle Cloud (2025)	6 millones de registros con identificadores biométricos	No constan

Comparativa entre tres métodos de suplantación de identidad: riesgo percibido y riesgo real

En esta tabla pueden verse las diferencias entre tres métodos de suplantación de identidad. Puede apreciarse una gran discrepancia entre el riesgo percibido por el público en general y el riesgo real.

Característica	Robo al responsable (Exfiltración BBDD)	Obtención en redes sociales (OSINT)	Ingeniería Social (Vishing/Phishing)
Origen del dato	Responsable del tratamiento	Redes sociales	La víctima
Naturaleza del dato	Plantilla matemática (Hash / Vector).	Imagen / Video	Datos suministrados por la víctima.
Estado técnico	Dato "muerto” (requiere ingeniería inversa).	Dato "vivo" (listo para procesar con IA).	Dato "en tiempo real" (máxima calidad).
Tasa de suplantación	0% conocida. No hay denuncias.	Alta (~70%). Crecimiento exponencial.	Extrema (~95%). El usuario "da permiso".
Denuncias reales	0 por suplantación (solo por privacidad).	Miles de denuncias (Deepfakes).	Millones de denuncias (Estafas).
Tipo de suplantación	Inyección de datos	Presentación	Presentación
Dificultad	Alta	Baja	Media
Escalabilidad	Baja (Múltiples barreras)	Muy alta (Se puede automatizar)	Individual (Muy laboriosa).
Uso de IA	Gran dificultad (Minimización de datos)	Clave. Permite crear Deepfakes.	Auxiliar. Mejora guiones y voces.
Interoperabilidad	Nula. El código robado no sirve en otro sistema.	Total. Una foto sirve para cualquier app.	Total. La víctima actúa en el sistema real.
Coste del ataque	Muy alto (hackear infraestructura).	Muy bajo (herramientas de IA gratis).	Variable (tiempo y manipulación).
Barreras de seguridad	Cifrado y algoritmos propietarios.	Ninguna. Datos publicados en RRSS.	La psicología y confianza humana.
Riesgo percibido por los usuarios y el público en general	Riesgo alto debido al desconocimiento	Riesgo bajo debido al desconocimiento	Riesgo bajo debido al desconocimiento
Riesgo real	Muy bajo o inexistente	Muy alto	Muy alto

ribas

Dificultades de la suplantación a través del robo de datos

El proceso de suplantación de identidad basado en el robo y el uso de datos biométricos tiene las siguientes dificultades.

Barreras de acceso	1. Segmentación de red y separación de servidores. 2. Firewalls. 3. Autenticación y privilegios.
Barreras de salida	1. Sistemas DLP. 2. Servidores Proxy y filtros de salida. 3. Datos señuelo.
Barrera de la irreversibilidad	1. Hash o vector matemático. 2. Proceso unidireccional. 3. Es matemáticamente imposible reconstruir la cara.
Barrera de la incompatibilidad	1. Cada fabricante utiliza su propio algoritmo. 2. Los datos no son compatibles con otros sistemas.
Barrera de la prueba de vida	1. Los sistemas actuales no aceptan imágenes estáticas. 2. Los sensores buscan pruebas que demuestren que el usuario que desea autenticarse es un usuario vivo. 3. A partir del hash no pueden generarse pruebas de vida.
Barrera del cifrado	1. Para usar un dato robado se debe inyectar el hash. 2. Los sistemas actuales rechazan los ataques de inyección.
Barrera de la inyección de datos	1. Para usar un dato robado se debe inyectar el hash. 2. Los sistemas actuales rechazan los ataques de inyección
Barrera de la autenticación multifactor	1. El dato biométrico va asociado a otro factor. 2. No puede haber autenticación 1:1 sin el otro factor.
Barrera de la caducidad	1. El patrón biométrico puede ser cancelado o revocado. 2. En caso de robo se pueden invalidar todos los hashes.
Barrera de la minimización	1. Los patrones utilizan el mínimo número de datos. 2. El detalle del patrón sería insuficiente para una reversión.
Barrera de la relación riesgo / recompensa	1. El riesgo de robar los datos biométricos es muy alto. 2. La recompensa es baja ya que el patrón obtenido es inútil.

ribas

Facilidad de la suplantación a través de una foto de redes sociales

El proceso de suplantación de identidad basado en la obtención de los datos biométricos a través de una foto o un vídeo publicado en las redes sociales y utilizando IA para la suplantación es mucho más fácil.

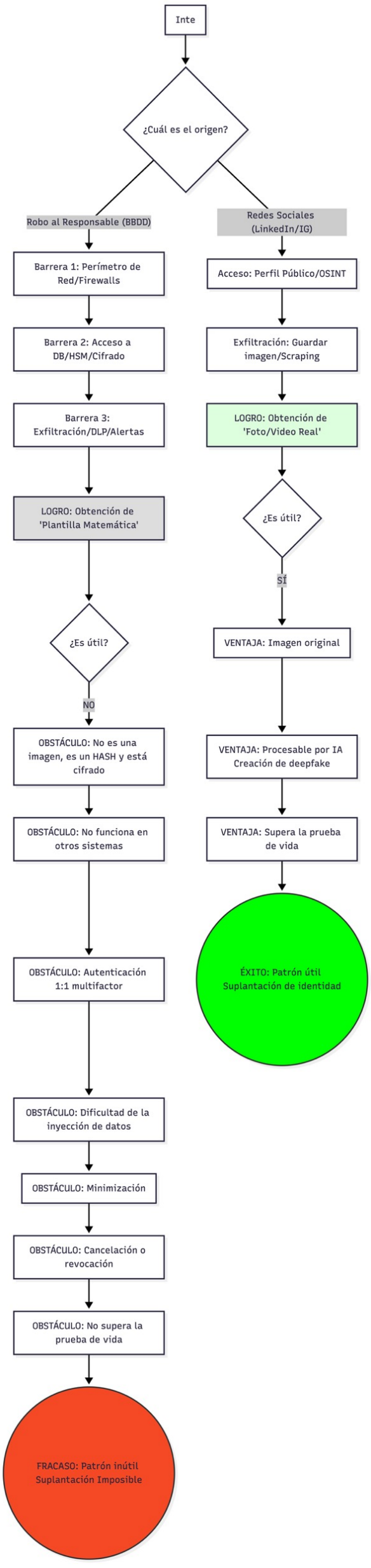
Barreras de acceso	1. No hay barreras de acceso. 2. Cualquier usuario puede acceder a una foto o un vídeo.
Barreras de salida	1. No hay barreras de salida. 2. Cualquier usuario puede descargar una foto o un vídeo.
Barrera de la irreversibilidad	1. Esta barrera no existe. 2. No hay hash.
Barrera de la incompatibilidad	1. Esta barrera no existe. 2. Los datos son totalmente compatibles.
Barrera de la prueba de vida	1. La muestra biométrica obtenida es suficiente. 2. La IA actuar puede simular pruebas de vida.
Barrera del cifrado	1. Esta barrera no existe. 2. Los datos no están cifrados.
Barrera de la inyección de datos	1. No es necesario inyectar datos. 2. Se trata de un ataque de presentación.
Barrera de la autenticación multifactor	1. El dato biométrico va asociado a otro factor. 2. No puede haber autenticación 1:1 sin el otro factor.
Barrera de la caducidad	1. Esta barrera no existe. 2. Los datos no pueden ser cancelados ni revocados.
Barrera de la minimización	1. Esta barrera no existe. 2. Los patrones utilizan el máximo número de datos.
Barrera de la relación riesgo / recompensa	1. El riesgo de la obtención de los datos es muy bajo. 2. La recompensa es alta ya que el patrón obtenido es útil.

Comparativa de barreras

En esta tabla se puede comprobar un contraste demoledor. Para el robo al responsable, el atacante debe ser un ingeniero experto enfrentándose a una fortaleza digital. Para la recolección en redes sociales, solo necesita ser un usuario medio con acceso a herramientas de IA comunes. Esto explica por qué las denuncias por suplantación desde redes sociales son masivas, mientras que desde bases de datos robadas son cero.

Barrera	Robo de datos biométricos	Obtención en redes sociales
Barrera de acceso	MUY ALTA	MUY BAJA
Barrera de salida	MUY ALTA	MUY BAJA
Barrera de la irreversibilidad	MUY ALTA	NO EXISTE
Barrera de la incompatibilidad	MUY ALTA	NO EXISTE
Barrera de la prueba de vida	MUY ALTA	BAJA
Barrera del cifrado	MUY ALTA	NO EXISTE
Barrera de la inyección de datos	MUY ALTA	NO ES NECESARIA
Barrera de la autenticación multifactor	ALTA	ALTA
Barrera de la caducidad	MUY ALTA	NO EXISTE
Barrera de la minimización	MUY ALTA	NO EXISTE
Barrera de la relación riesgo / recompensa	Riesgo muy alto Recompensa inexistente	Riesgo muy bajo Recompensa alta

ribas



Comparativa de procesos

En este diagrama de flujo pueden verse los obstáculos que un experto va a encontrar en el camino a la suplantación de identidad a partir del robo de datos biométricos al responsable del tratamiento.

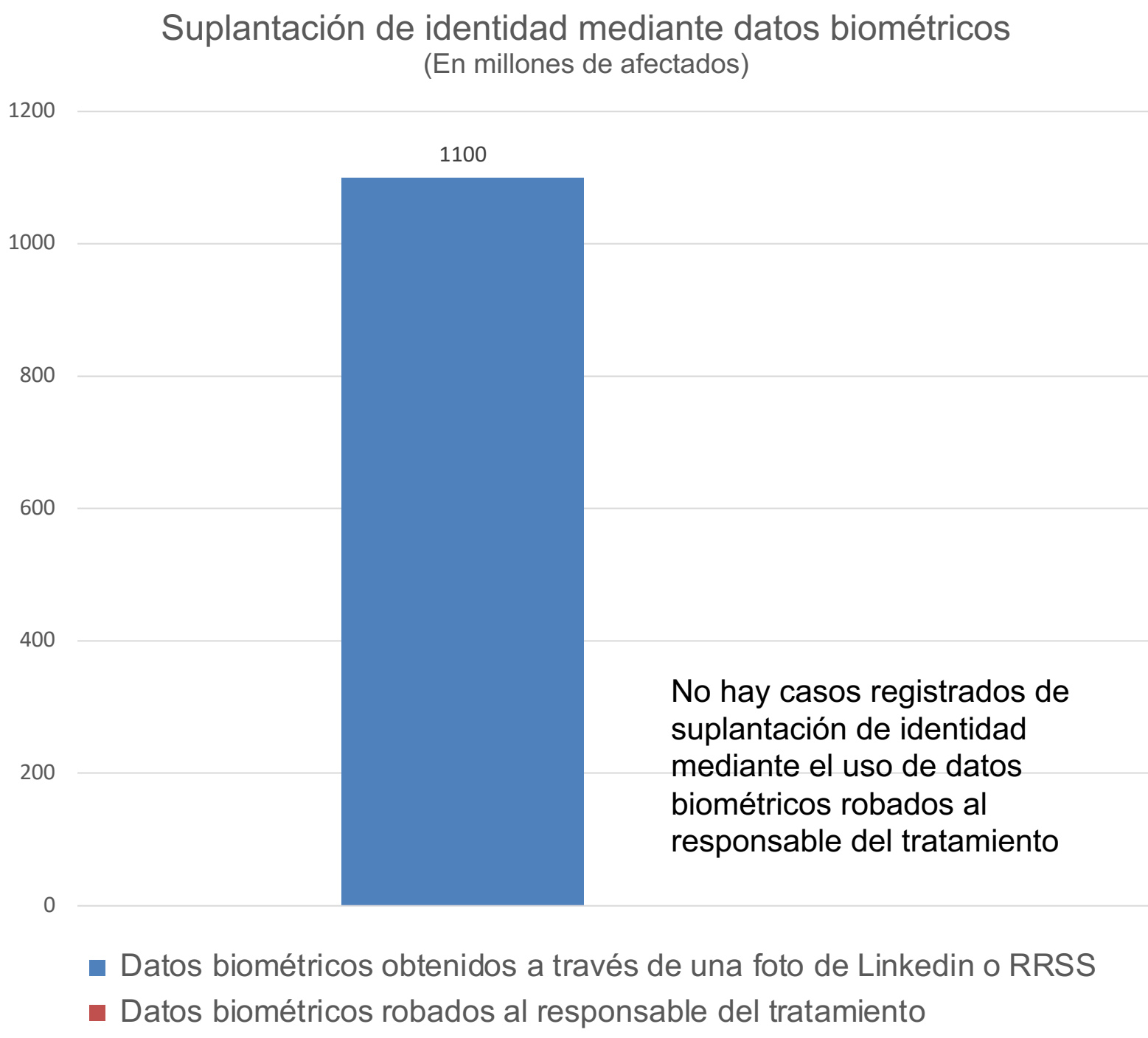
También puede verse el camino llano hacia el mismo objetivo a partir de la obtención de datos biométricos mediante una fotografía o un vídeo publicado por la víctima en LinkedIn o en una red social como Facebook o Instagram, utilizando herramientas gratuitas y sin necesidad de ser un experto.

Esto explica por qué las denuncias por suplantación desde redes sociales son masivas, mientras que desde bases de datos robadas son cero.

ribas

Casos de suplantación de identidad

En este gráfico puede verse que las estadísticas relativas a la suplantación de identidad mediante el uso de datos biométricos de la persona suplantada demuestran que el uso de datos robados es prácticamente inexistente.



ribas

Casos de suplantación de identidad a partir de datos biométricos robados o expuestos

La leyenda urbana en la que se sustentan los argumentos de las autoridades de control está basada en la creencia de que, si los datos biométricos que gestiona el responsable del tratamiento son robados o expuestos en una brecha de seguridad, el interesado podrá ser víctima de una suplantación de identidad. Según las estadísticas mundiales sobre la materia, esta creencia está infundada, ya que, de un total de más de 300 millones de personas afectadas por incidentes de seguridad relacionados con datos biométricos, ninguno de ellos ha presentado una queja o una denuncia.

Las autoridades de control consideran la ausencia de quejas y denuncias como un indicador importante en la decisión de archivar la investigación de una brecha de seguridad, incluso en el caso de que los datos hayan sido publicados.

Más de 1.000 millones de afectados
vs.
Cero denuncias

ribas

Casos de suplantación de identidad a partir de datos biométricos obtenidos a través de fotos de redes sociales

Los datos relativos a este tipo de suplantaciones son relevantes:

1. Crecimiento del 3.000% de los ataques con deepfakes.
2. El 71% de los usuarios no sabe identificar un deepfake biométrico.
3. 1,4 millones de denuncias en EEUU según la FTC en el periodo 2024 -2025

La disponibilidad de imágenes en fuentes abiertas y la facilidad de obtener datos biométricos a través de ellas genera actualmente un riesgo de suplantación mucho probable, fácil y perjudicial que el robo de bases de datos almacenadas en los sistemas del responsable del tratamiento.

Caso Arup - Ataque mediante deepfake de IA

Año	2024
Víctima	Filial en Hong Kong de Arup, empresa global de ingeniería con sede en Londres
Tipo de ataque	Suplantación de directivos mediante ataque de presentación con deepfake
Mecánica del ataque	1. Videollamada con deepfake en tiempo real que suplantaba al CFO. 2. En la videollamada participaban otros deepfake de directivos. 3. El empleado creyó estar viendo al director financiero y autorizó los pagos.
Datos biométricos	Sí, obtenidos a partir de las fotos y vídeos del director financiero y otros.
Uso de sistema de IA	Sí, para crear un deepfake en tiempo real a partir de los datos biométricos.
Resultado	15 transferencias que sumaron 25,6 millones de dólares
Origen de los datos	Fotos y vídeos de los directivos publicados en LinkedIn y en YouTube.
Dificultad del ataque	Muy baja: Herramientas de bajo coste + investigación en LinkedIn.

Otros casos de obtención de datos biométricos a través de fotos de redes sociales

En esta tabla se resumen casos similares de obtención de datos biométricos a través de fotos publicadas en redes sociales.

Caso	Metodología	Resultados
Clearview AI	Scraping masivo de imágenes en redes sociales.	Obtención de más de 30.000 millones de imágenes de redes sociales (LinkedIn, Facebook, Instagram) para entrenar algoritmos de reconocimiento facial.
KnowBe4	El atacante utilizó fotos de alta calidad de una persona real encontradas en redes profesionales para construir su avatar digital clonado.	Una empresa de ciberseguridad contrató al avatar clonado por el atacante que usó una el deepfake en tiempo real durante la entrevista.
Caso Ana	Los atacantes utilizaron fotos frontales de sus perfiles públicos para superar las verificaciones biométricas sencillas de las operadoras (que solo pedían una foto estática o un parpadeo).	Suplantación de la identidad para contratar 11 líneas telefónicas con las que se realizaron múltiples estafas.

Estadísticas sobre suplantación de identidad

En esta tabla se hace una breve referencia a los datos estadísticos disponibles para el periodo 2024 - 2025. En ninguno de ellos se han utilizado patrones biométricos robados al responsable del tratamiento.

Metodología	Datos y denuncias
Deepfakes biométricos	Según Identity Fraud Report de 2025, los intentos de suplantación mediante deepfakes biométricos creados a partir de fotos y vídeos publicados en redes sociales ocurren a un ritmo de uno cada cinco minutos a nivel global.
Fotos de redes sociales DNI escaneados en falsas ofertas de empleo	Según INCIBE, en 2024 se registraron 7.712 denuncias específicas de suplantación de identidad solo en el sector del juego online (Protocolo PACS). La mayoría de estas víctimas denunciaron que sus fotos de redes sociales o DNI escaneados en falsas ofertas de empleo fueron usados para crear cuentas.
	El INCIBE reportó que un 14% de los internautas españoles sufrió algún tipo de suplantación de identidad digital en el último año, siendo la duplicación de perfil con fines fraudulentos, usando fotos de Instagram/LinkedIn la modalidad más denunciada.
	El reporte de Veriff 2025 indica que 1 de cada 20 intentos de verificación de identidad en el sector financiero ya es fraudulento, y el 40% de esos fraudes son ataques de presentación, mediante fotos o vídeos obtenidos de redes sociales.
	1.4 millones de denuncias en EE.UU según la FTC relacionados con la suplantación de identidad con datos biométricos obtenidos a través de las fotos y los vídeo publicados en las redes sociales.

Tasa de éxito

En la siguiente tabla puede verse una comparativa de la tasa de éxito de cada modalidad de ataque de obtención de datos y suplantación de identidad:

Metodología	Tasa de éxito estimada	Razón del éxito o el fracaso
Robo de datos biométricos al responsable del tratamiento.	Baja o inexistente	Las plantillas robadas suelen estar en formatos propietarios o hashes que no pueden reinyectarse fácilmente en otros sistemas.
Obtención de datos biométricos a través de fotos obtenidas en redes sociales.	Muy alta	Las fotos y videos descargados permiten crear deepfakes. En 2025, 1 de cada 20 rechazos en la verificación de identidad bancaria fue un deepfake realizado con IA.
Obtención de datos biométricos a través de videoconferencias.	Muy alta	La obtención de datos biométricos a través de videoconferencias permite crear avatares muy precisos.

Ataque de inyección vs. ataque de presentación

No se han localizado evidencias de que un ataque de inyección de plantilla biométrica robada haya prosperado y haya escalado a un fraude masivo, mientras que los ataques de presentación de deepfake a partir de datos obtenidos en redes sociales causaron pérdidas millonarias documentadas en 2024 y 2025.

En esta tabla se pueden ver las diferencias entre ambos tipos de ataque.

Ataque de Inyección A partir del robo de datos biométricos al responsable del tratamiento	El atacante intenta introducir el código binario robado directamente en el flujo de datos del sistema. Es mucho más difícil que el ataque de presentación porque requiere una manipulación experta de la aplicación de destino, no solo tener el dato biométrico. Además, hay que superar un gran número de barreras técnicas, como hemos visto.	No se han reportado casos
Ataque de Presentación A partir de la obtención de los datos biométricos a través de fotos obtenidas en redes sociales	El atacante utiliza una foto de LinkedIn o de otras redes sociales, la anima con IA y la pone frente a la cámara del móvil. Es el método más común en los fraudes actuales.	Ha sido la técnica más utilizada y más letal en 2024 y 2025. Existen miles de casos documentados, además de los grandes casos corporativos comentados.

Obtención de datos biométricos en entrevistas laborales falsas

La trampa biométrica basada en una entrevista laboral falsa es un método muy eficaz, que ha generado muchas denuncias en 2025. En este caso el atacante captura de forma directa los datos biométricos de la víctima.

La mecánica es la siguiente:

1. El atacante crea una falsa oferta de empleo en LinkedIn.
2. Durante la entrevista por videoconferencia, el atacante pide al usuario que realice movimientos faciales o escanee su DNI para validar su perfil.
3. Con esos datos vivos capturados directamente de la víctima y no robados de un servidor, el atacante abre cuentas bancarias o pide préstamos.

Los casos de suplantación reportados a causa de esta técnica son menos numerosos que los relacionados con la obtención de datos biométricos a través de fotos y vídeos publicados en redes sociales, como puede verse en esta tabla.

Origen de los datos biométricos	Casos de suplantación reportados
Robo de los datos biométricos al responsable del tratamiento.	0
Obtención de datos biométricos a través de fotos y vídeos publicados en redes sociales.	Miles - Crecimiento del 3.000%
Entrevistas laborales falsas.	Más de 35

Irreversibilidad

En la resolución de la AEPD en el caso de AENA se menciona el riesgo de reversión no autorizada de los datos biométricos que permita la reidentificación del interesado aparece como un atributo que AENA considera acreditado y propio de la inmensa mayoría de los sistemas biométricos del mercado.

La capacidad de los sistemas biométricos de evitar la reversión de los datos biométricos y la reidentificación del interesado no es una materia controvertida en la resolución.

Los responsables del tratamiento no guardan imágenes de la huella dactilar o de la cara, sino representaciones matemáticas. Reconstruir una cara física a partir de un código binario robado es actualmente una imposibilidad técnica para la mayoría de los sistemas comerciales.

Cifrado

En conexión con la prevención del riesgo de reversión y reidentificación en la resolución de la AEPD en el caso de AENA en la EIPD también se considera acreditado la existencia del cifrado.

La existencia y la idoneidad del cifrado no es una materia controvertida en la resolución.

Incompatibilidad

Cada fabricante utiliza un algoritmo propietario y una configuración de hash diferente para cada cliente, por o que un patrón biométrico robado de la base de datos de una empresa no sirve para entrar en el sistema de otra empresa.

ribas

Alternativas al control biométrico

Búsqueda de sistemas de autenticación que sean equivalentes y menos invasivos que el control de acceso con datos biométricos

Clasificación del ENS

Siguiendo la clasificación del Esquema Nacional de Seguridad y la evaluación posterior realizada por el CCN, se analizan a continuación las tres categorías de factores de autenticación.

Nivel	Atributo	Factor de autenticación
Nivel 1	Conocimiento	Algo que el usuario sabe
Nivel 2	Posesión	Algo que el usuario tiene
Nivel 3	Inherencia	Algo que el usuario es

Factores de autenticación

Nivel 1

Conocimiento - Algo que el usuario sabe

Ejemplos:

1. Contraseña.
2. PIN.
3. Secreto.
4. Frase de seguridad.
5. Respuestas a preguntas de seguridad.
6. Patrón de desbloqueo en pantalla táctil.

Riesgos:

1. Puede ser robado.
2. Puede ser cedido por el usuario a un tercero sin derechos de acceso.

Factores de autenticación

Nivel 2

Posesión - Algo que el usuario tiene

Ejemplos:

1. Código recibido por SMS
2. Código QR
3. Token
4. Aplicación de autenticación
5. Tarjeta de acceso
6. DNI o pasaporte
7. Llave física USB
8. Certificado digital - DNI electrónico

Riesgos:

1. Puede ser robado.
2. Puede ser cedido por el usuario a un tercero sin derechos de acceso.

Factores de autenticación

Nivel 3

Posesión - Algo que el usuario es

Ejemplos:

1. Huella dactilar.
2. Cara.
3. Iris o retina.
4. Voz.
5. Geometría de la mano.
6. Patrón venoso.
7. Patrón de tecleo.
8. Firma manuscrita biométrica.
9. Comportamiento y movimiento.

Ventajas:

1. No puede ser robado y explotado con eficacia.
2. No puede ser cedido por el usuario a un tercero sin derechos de acceso.

Evaluación realizada por el CCN

El Centro Criptológico Nacional (CCN) ha evaluado exhaustivamente las tecnologías biométricas para el control de acceso, destacando su eficacia en términos de seguridad y privacidad.

En su documento CCN-TEC 013, el CCN recomienda el uso de sistemas de control de acceso basados en plantillas biométricas Renewable Biometric References (RBR) para entornos que requieren un alto nivel de seguridad.

Estas plantillas ofrecen características como inherencia, irreversibilidad, revocabilidad y no interoperabilidad, impidiendo la suplantación de identidad y mejorando la protección de los datos personales.

Inexistencia de sistemas equivalentes

El CCN señala que la biometría garantiza que la identidad sea real, superando las limitaciones de factores de posesión o conocimiento que permitiría a otros sistemas de autenticación ser cedidos o sustraídos por terceros.

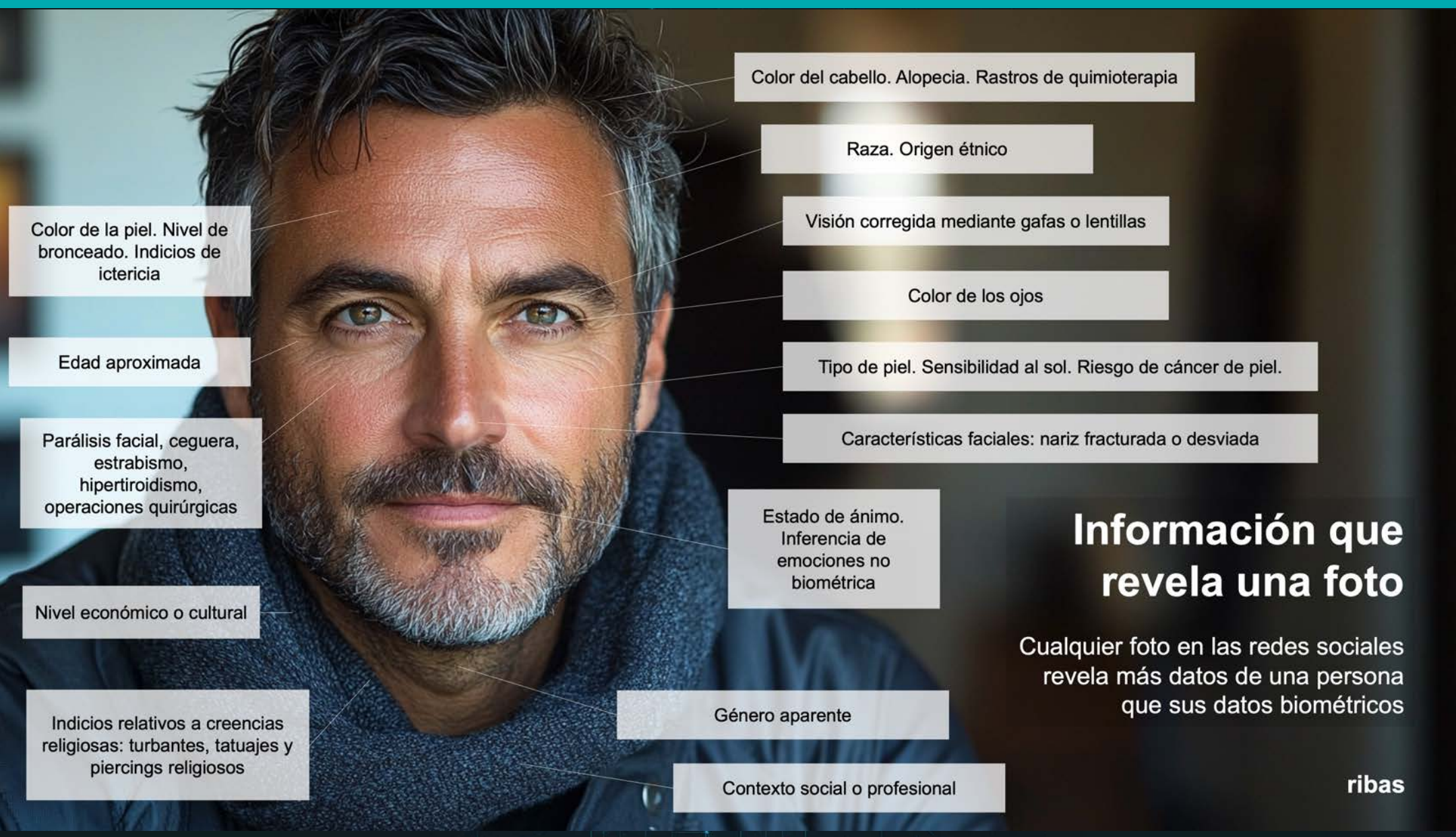
El factor de inherencia de la biometría ofrece garantías únicas que refuerzan la protección contra el fraude y la suplantación de identidad, sin encontrar una alternativa equivalente en otros medios.

Conclusión

De acuerdo con la información facilitada por el CCN, no existe un sistema de autenticación equivalente y menos intrusivo.

Datos biométricos sobrevalorados

Los datos biométricos dedicados a la autenticación presencial generan mucho menos riesgo para el interesado que una simple foto publicada en las redes sociales.



Información que revela un dato biométrico

Los puntos de referencia de una plantilla biométrica se limitan a los necesarios para conseguir verificar la identidad del interesado

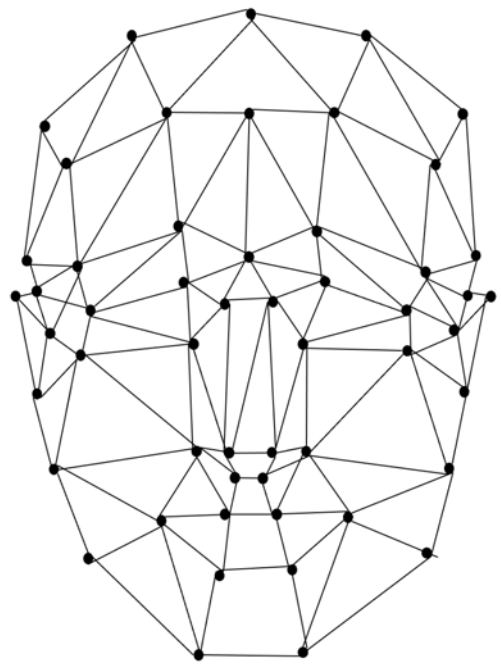
• •

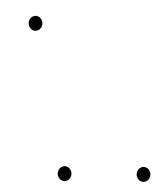
El interesado es, o no es, quien dice ser

ribas

Efectos de la minimización extrema

Los puntos de referencia de una plantilla biométrica se limitan a los necesarios para conseguir verificar la identidad del interesado





Lo que muchas personas piensan

Los datos biométricos han sido demonizados a causa de la creencia en riesgos asociados a la suplantación de la personalidad y a la obtención de datos de salud o las emociones

Lo que las empresas tratan

Las empresas únicamente tratan el número mínimo de puntos de referencia para verificar la identidad de una persona en una comunidad pequeña de usuarios. Por ejemplo, 4 puntos para un grupo de 1000 personas.

Datos que puede revelar una fotografía y los datos biométricos destinados al control de acceso

En esta tabla se comparan los datos que puede revelar una simple fotografía y los que puede revelar una plantilla biométrica destinada al control de acceso

Datos que se pueden obtener a través de una foto o un vídeo	Datos que se pueden obtener a través los datos biométricos
Raza - Origen étnico	El interesado es, o no es, quien dice ser
Género aparente	
Contexto social o profesional	
Peso aproximado - Enfermedades o afecciones: anorexia, obesidad	
Vista corregida mediante gafas	
Color de la piel, nivel de bronceado, indicios de ictericia	
Color de los ojos	
Color del cabello	
Alopecia, rastros de quimioterapia	
Tipo de piel, sensibilidad al sol y riesgo de cáncer de piel	
Edad aproximada	
Estado anímico	
Tatuajes y piercings	
Indicios relativos a creencias religiosas: turbantes, tatuajes y piercings religiosos	
Características de la piel: arrugas, pecas y lunares, melanoma, textura, flacidez	
Características faciales: nariz fracturada, nariz desviada, orejas muy grandes…	
Parálisis facial, ceguera, estrabismo, hipertiroidismo, operaciones quirúrgicas…	
Y un largo etcétera	

ribas

Los datos biométricos después de un ciberataque

Los datos biométricos dedicados a la autenticación presencial generan mucho menos riesgo para el interesado después de un ciberataque que una simple foto publicada en las redes sociales.

ribas

Plantillas anónimas para terceros

Las plantillas biométricas actuales están seudonimizadas, es decir, su vinculación con un interesado concreto únicamente es conocida por el responsable del tratamiento y la información que permite establecer esta asociación está en otro sistema, por lo que un eventual atacante accedería a datos que no podría atribuir al interesado.

ribas

Plantillas incompatibles

Las plantillas biométricas actuales son incompatibles con otros sistemas, por lo que un eventual atacante no podría utilizarlas.

ribas

Datos insuficientes

De acuerdo con el principio de minimización, las plantillas biométricas actuales únicamente incluyen la información estrictamente necesaria para verificar que el interesado es quien dice ser. Esta finalidad puede conseguirse con menos de 8 puntos de referencia de la cara o la huella dactilar. Con tan escasa información, no se pueden inferir otros datos del interesado y mucho menos datos de salud.

Datos irreversibles

Las plantillas biométricas actuales tienen se basan en un hash que hace que los datos sean irreversibles. El modelo matemático del hash y la minimización de datos hacen imposible volver al original mediante ingeniería inversa.

ribas

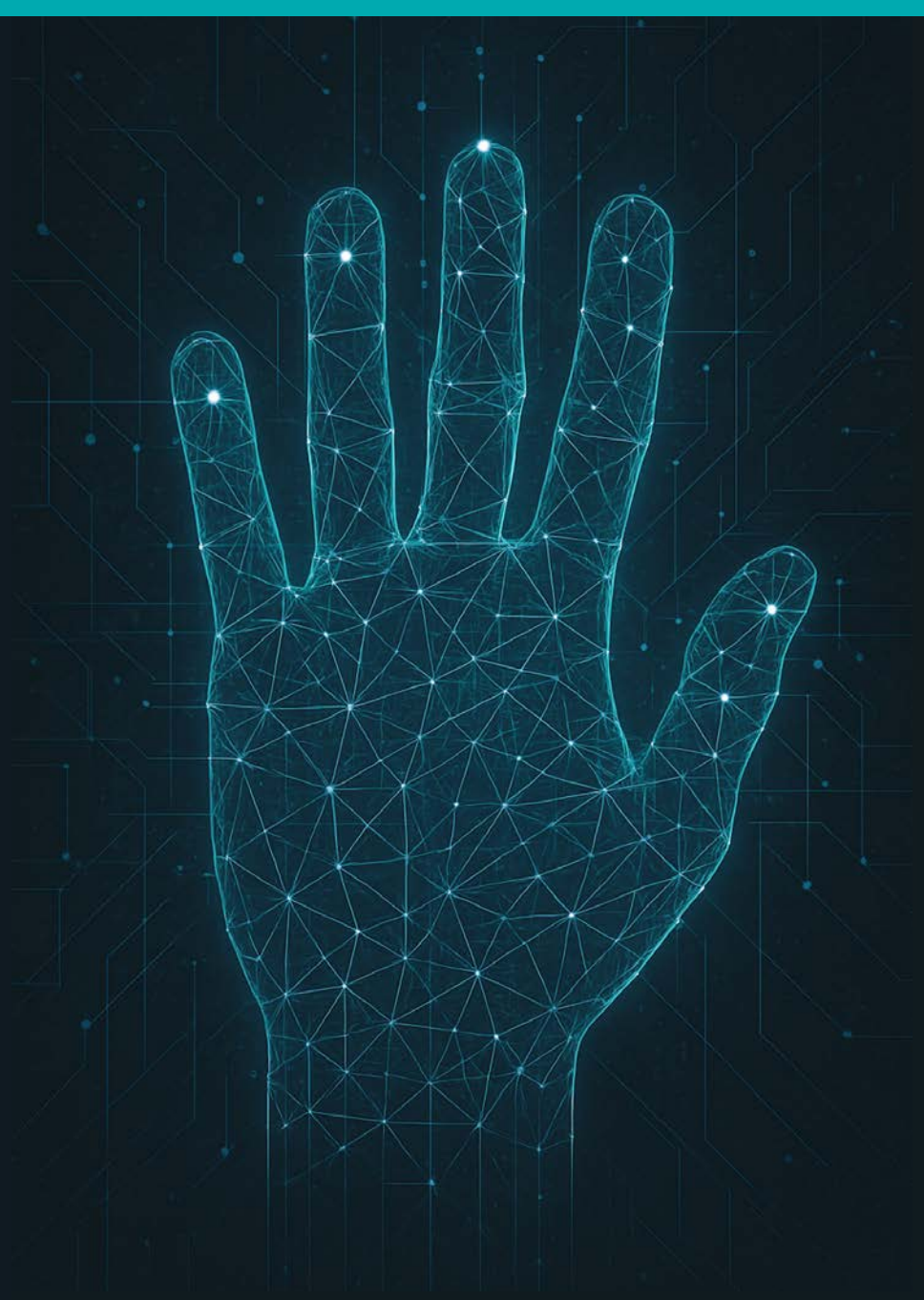
Datos revocables

Después de un ciberataque las plantillas biométricas actuales pueden ser revocadas de tal manera que el sistema no las podrá reconocer. Al incluir tan pocos puntos de referencia, una plantilla biométrica puede ser sustituida por otra plantilla con otros puntos de referencia distintos de los anteriores.

ribas

Datos biométricos que no van dirigidos a identificar a una persona

Y que, por lo tanto, no cumplen el requisito de la finalidad establecido en el artículo 9.1 del RGPD



ribas

Tratamientos de datos biométricos con finalidades médicas

Datos biométricos	Finalidad	¿Permite la identificación o autenticación del interesado?	¿Va dirigido a la identificación del interesado?
Patrón de sueño	Detección de la apnea	Sí	No
Patrón de actividad cerebral	Detección de lesiones	Sí	No
Patrón de pisada o marcha	Prevención de lesiones	Sí	No
Patrón de impacto articular	Prevención de lesiones	Sí	No
Patrón respiratorio	Monitorización clínica	Sí	No
Patrón cardíaco	Monitorización clínica	Sí	No
Patrón de movimientos musculares	Rehabilitación física	Sí	No
Patrón del iris	Diagnóstico precoz	Sí	No
Patrón de la retina	Diagnóstico precoz	Sí	No
Patrón de la mácula	Diagnóstico precoz	Sí	No
Patrón de movimiento ocular (Eye-tracking)	Evaluación del deterioro cognitivo	Sí	No
Patrón de voz	Diagnóstico precoz de enfermedades neurológicas como Parkinson o Alzheimer	Sí	No
Patrón facial	Inferencia de emociones en psicología y psiquiatría	Sí	No

Tratamientos de datos biométricos con finalidades deportivas y de bienestar

Datos biométricos	Finalidad	¿Permite la identificación o autenticación del interesado?	¿Va dirigido a la identificación del interesado?
Patrón postural	Fisioterapia y PRL	Sí	No
Patrón de fatiga y estrés muscular	Mejora del rendimiento	Sí	No
Patrón de saturación de oxígeno	Entrenamiento deportivo	Sí	No
Patrón de HRV	Entrenamiento deportivo	Sí	No
Patrón de temperatura corporal	Entrenamiento y PRL	Sí	No
Patrón aeróbico y anaeróbico	Entrenamiento y PRL	Sí	No
Patrón biomecánico y articular	Prevención de lesiones	Sí	No
Patrón de centro de masas y equilibrio	Prevención de caídas	Sí	No
Patrón de pisada y marcha	Prevención de lesiones	Sí	No
Patrón compensatorio	Prevención de lesiones	Sí	No
Patrón glucógeno y de consumo calórico	Mejora del rendimiento	Sí	No
Patrón de hidratación	Mejora del rendimiento	Sí	No

Tratamientos de datos biométricos con finalidades de interacción con sistemas (HCI/UX)

Datos biométricos	Finalidad	¿Permite la identificación o autenticación del interesado?	¿Va dirigido a la identificación del interesado?
Patrón de movimiento	Reconocimiento de gestos asignados a acciones	Sí	No
Patrón de movimiento ocular (Eye-tracking)	Seguimiento ocular en una página web para mejorar la experiencia de usuario.	Sí	No
Patrón facial	Inferencia de emociones para adaptar los contenidos en educación o videojuegos	Sí	No
Patrón de tecleo	Mejora de la accesibilidad y personalización	Sí	No
Patrón de uso del ratón	Mejora de la accesibilidad y personalización	Sí	No

Tratamientos de datos biométricos con finalidades de simulación, virtualización o entretenimiento

Datos biométricos	Finalidad	¿Permite la identificación o autenticación del interesado?	¿Va dirigido a la identificación del interesado?
Patrón facial	Creación de avatares para formación o videojuegos. Inferencia de emociones para adaptar los contenidos en educación o videojuegos. Aplicación de filtros o efectos en redes sociales.	Sí	No
Patrón de voz	Clonación de la voz	Sí	No
Patrón de movimiento	Reconocimiento de gestos asignados a acciones en simuladores y videojuegos	Sí	No
Patrón de movimiento ocular (Eye-tracking)	Seguimiento ocular para guiar el movimiento en simuladores y videojuegos	Sí	No

Tratamientos de datos biométricos con finalidades contractuales, de autenticación, de consentimiento o de seguridad

Datos biométricos	Finalidad	¿Permite la identificación o autenticación del interesado?	¿Va dirigido a la identificación del interesado?
Firma biométrica	Muestra de consentimiento Aceptación de contrato	Sí	No
Patrón facial	Acceso a sistemas o instalaciones	Sí	No
Patrón dactiloscópico	Acceso a sistemas o instalaciones	Sí	No
Patrón de voz	Acceso a sistemas o instalaciones	Sí	No
Patrón de iris	Acceso a sistemas o instalaciones	Sí	No
Patrón de la palma de la mano	Acceso a sistemas o instalaciones	Sí	No

Estos ejemplos demuestran que la regulación de los datos biométricos en el RGPD se divide en estos dos subconjuntos.

Diferencia entre el artículo 4.14 y el 9.1 del RGPD

Artículo 4.14 **Definición de dato biométrico**	**Artículo 9.1** **Datos biométricos prohibidos**
Capacidad	Finalidad
Que permitan o confirmen la identificación única de dicha persona	Datos biométricos dirigidos a identificar de manera unívoca a una persona física
Incluye todos los datos biométricos que no persigan la finalidad de identificar de manera unívoca a una persona física	Incluye únicamente los datos biométricos que persigan la finalidad de identificar de manera unívoca a una persona física

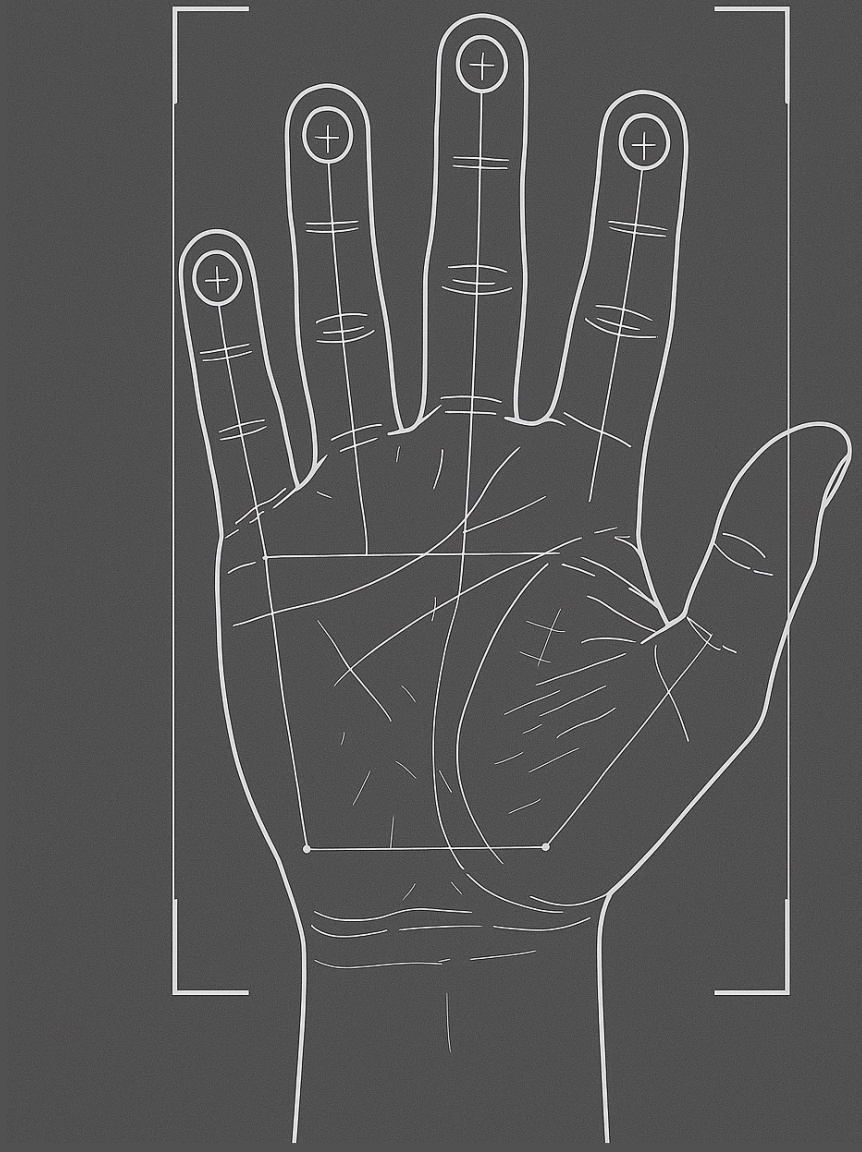
ribas

Conclusión

Cuando el artículo 9.1 incluye en las categorías especiales de datos los "datos biométricos dirigidos a identificar de manera unívoca a una persona física" indica claramente que en el RGPD puede haber otros datos biométricos que no tengan esta finalidad.

Datos biométricos y derechos fundamentales

Afectación de las categorías especiales de datos del artículo 9.1 del RGPD a los derechos y libertades fundamentales



ribas

Afectación de derechos y libertades fundamentales

Análisis de la afectación de los principales derechos y libertades fundamentales a través del tratamiento de las categorías especiales de datos del artículo 9.1 del RGPD. Al tener un carácter instrumental, la autenticación biométrica no tiene la misma afectación.

Derecho o libertad fundamental	Origen étnico o racial	Opiniones políticas	Convicciones religiosas	Datos genéticos	Salud	Orientación sexual	Identificación biométrica sin participación activa	Autenticación biométrica
Derecho a la vida								
Libertad ideológica y religiosa								
Libertad								
Honor e intimidad								
Inviolabilidad domicilio								
Secreto comunicaciones								
Libertad residencia y deambulatoria								
Libertad de expresión								
Reunión, asociación y sufragio								
Igualdad								
Educación								
Función pública								
Presunción de inocencia								

ribas

Conclusiones de la tabla

Como puede verse en la tabla, no todas las categorías especiales de datos del artículo 9.1 del RGPD tienen el mismo impacto y generan los mismos riesgos para los derechos y libertades de los interesados.

La última columna de la tabla demuestra que la verificación biométrica (1:1) tiene un impacto inferior.

Uso instrumental

Además, el riesgo lo genera la aplicación directa de las categorías especiales de datos y no su uso instrumental. Por ejemplo, una persona puede ser discriminada por su origen étnico. Pero en el caso de la autenticación biométrica, un alumno no será expulsado de un examen online por sus datos biométricos, sino por cometer fraude.

Es decir, existe una finalidad principal de prevención del fraude, y los sistemas biométricos son una medida instrumental para cumplir esa finalidad.

Los datos biométricos en la doctrina del Tribunal Supremo

Importantes argumentos a favor de la no afectación de derechos fundamentales en el uso de una plantilla biométrica con minimización extrema y participación activa del interesado.

ribas

Minimización extrema

“La imagen de la mano acaba convertida en un registro de nueve bytes válido para, mediante un tratamiento informático que lo relaciona con otros datos, y así identificar a los empleados públicos del Gobierno de Cantabria y así controlar el cumplimiento del horario de trabajo.”

No afectación de derechos fundamentales

Este tratamiento “no responde al patrón de las intromisiones ilegítimas en la esfera de la intimidad, tanto por la parte del cuerpo utilizada, como por las condiciones en que se usa”.

Plantilla seudonimizada

“La plantilla no comporta huellas, ni fotografías y, por sí sola, no es idónea para identificar a las personas”.

“Solamente se incluyen elementos binarios codificados en nueve bytes de modo que, a partir de ellos, no es posible establecer la identidad de una persona”.

No invasión de la intimidad

El tratamiento se considera intrascendente desde la perspectiva del artículo 18.1 de la Constitución Española.

Base jurídica

“La finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento”.

Roj: **STS 5200/2007** - **ECLI:ES:TS:2007:5200**

Id Cendoj: **28079130072007100789**
Órgano: **Tribunal Supremo. Sala de lo Contencioso**
Sede: **Madrid**
Sección: **7**
Fecha: **02/07/2007**
Nº de Recurso: **5017/2003**
Nº de Resolución:
Procedimiento: **RECURSO CASACIÓN**
Ponente: **PABLO MARIA LUCAS MURILLO DE LA CUEVA**
Tipo de Resolución: **Sentencia**

Resoluciones del caso: **STS 5200/2007,**
STSJ CANT 348/2003

Esta sentencia es previa al RGPD, pero contiene una valoración de la intrascendencia de una plantilla biométrica minimizada para los derechos fundamentales, especialmente en relación con la intimidad y el artículo 18.1 de la Constitución Española. También es importante la referencia a la base jurídica. Estos argumentos están plenamente vigentes en la actualidad y son compatibles con el RGPD.

Conclusiones

De esta sentencia sobre control horario biométrico podemos extraer conclusiones que son perfectamente compatibles con el régimen actual del RGPD:

1. La plantilla biométrica no contiene huellas ni fotografías.
2. Solamente se incluyen elementos binarios codificados en 9 bytes, de modo que, a partir de ellos, no es posible establecer la identidad de una persona.
3. Ello significa que la plantilla por sí sola no es idónea para identificar a las personas.
4. La conexión con la persona proviene del acto de relacionar la plantilla con otros datos.
5. Estos datos serían las plantillas previamente obtenidas en el registro de las personas.
6. Se trataría por lo tanto de un supuesto de identificación biométrica (1:n), presencial y con participación activa del interesado, que en el RIA también queda fuera de la zona de alto riesgo.
7. Este tratamiento no responde al patrón de las intromisiones ilegítimas en la esfera de la intimidad.
8. El tratamiento se considera intrascendente desde la perspectiva del artículo 18 de la Constitución Española.
9. La finalidad perseguida por el tratamiento es plenamente legítima.
10. Esta finalidad sería el control del cumplimiento de las obligaciones legales y contractuales por parte del interesado.
11. Estas obligaciones son inherentes a la relación que une al interesado con el responsable del tratamiento, por lo que no es necesario obtener previamente su consentimiento.

Esta última aportación abriría la puerta a aplicar la base jurídica del artículo 6.1.b del RGPD (ejecución de un contrato) y permitiría reforzar la excepción de la obligación legal de cumplir el horario por parte del trabajador prevista en el artículo 9.2.b.

Finalmente, se refuerza la tesis de que el tratamiento de los datos biométricos es instrumental y se configura como un subtratamiento del tratamiento principal, que en este caso es el control horario y la verificación del cumplimiento del contrato.

El error humano en la verificación manual de la identidad

Mayor fiabilidad de los datos biométricos en el control de acceso y la verificación de la identidad.

ribas

Factor humano y brechas de seguridad

El factor humano es la principal causa de las violaciones de la seguridad de los datos y de la ineficacia de las medidas de seguridad

ribas

Error humano en la verificación manual de la identidad

Se estima que el error humano en la verificación manual de la identidad es superior al 10%

ribas

Mayor fiabilidad de los sistemas biométricos

Tasas de falsos positivos por debajo de 0.000001 (Fuente: CCN)

Es decir, sólo un 0.0001% de las veces el sistema biométrico confunde a dos personas diferentes indicando que son la misma persona. (Fuente: CCN)

Tasas de falsos negativos inferiores a 0.005. (Fuente: CCN)

Es decir, sólo el 0,5% de las personas legítimas son rechazadas de forma incorrecta. (Fuente: CCN)

ribas

Riesgo residual insalvable

A pesar de todas las medidas aplicadas para su predicción (Técnica THERP) y reducción (Técnica SHERPA), siempre existe un riesgo residual de error insalvable, tal como indica el Ministerio de Trabajo en su nota técnica sobre los métodos de análisis de la fiabilidad humana.

ribas

Errores de percepción y comparación

Causas:

1. Similitud con otra persona.
2. Similitud de rasgos entre familiares.
3. Similitud de rasgos raciales. Este error es relevante en las empresas con trabajadores extranjeros.
4. Cambios físicos: barba, maquillaje, cambios en el peso, envejecimiento.
5. Fatiga visual, estrés, cansancio, alta frecuencia o excesiva velocidad de los reconocimientos.

Errores por falta de atención

Causas:

1. No revisar con detenimiento los rasgos faciales por prisa o rutina.
2. Pasar por alto pequeños detalles (cicatrices, lunares, asimetrías).
3. No comparar con suficiente tiempo la foto con el rostro real.
4. Distraerse con otros elementos del documento (fecha de nacimiento, nombre) y no centrarse en la imagen.

Errores debido a sesgos cognitivos

Causas:

1. Sesgo de comparación: confianza excesiva en una característica facial.
2. Sesgo de confirmación: Si el verificador cree que la persona es legítima, puede pasar por alto discrepancias.
3. Efecto de familiaridad: Si el individuo parece "confiable", el agente puede no revisar con la misma rigurosidad.
4. Discriminación inconsciente: Algunas personas pueden recibir más escrutinio que otras según su apariencia.

ribas

Errores del ser humano en la autenticación manual

Resumen

Tipo de error	Ejemplos
1. Errores de percepción y comparación	1. Similitud con otra persona. 2. Similitud de rasgos entre familiares. 3. Similitud de rasgos raciales. Este error es relevante en las empresas con trabajadores extranjeros. 4. Cambios físicos: barba, maquillaje, cambios en el peso, envejecimiento. 5. Fatiga visual, estrés, cansancio, alta frecuencia o excesiva velocidad de los reconocimientos.
2. Errores por falta de atención	1. No revisar con detenimiento los rasgos faciales por prisa o rutina. 2. Pasar por alto pequeños detalles (cicatrices, lunares, asimetrías). 3. No comparar con suficiente tiempo la foto con el rostro real. 4. Distraerse con otros elementos del documento (fecha de nacimiento, nombre) y no centrarse en la imagen.
3. Errores debido a sesgos cognitivos	1. Sesgo de comparación: confianza excesiva en una característica facial. 2. Sesgo de confirmación: Si el verificador cree que la persona es legítima, puede pasar por alto discrepancias. 3. Efecto de familiaridad: Si el individuo parece "confiable", el agente puede no revisar con la misma rigurosidad. 4. Discriminación inconsciente: Algunas personas pueden recibir más escrutinio que otras según su apariencia.

Mayor fiabilidad de los sistemas biométricos

Tasas de falsos positivos por debajo de 0.000001 (Fuente: CCN)

Es decir, sólo un 0.0001% de las veces el sistema biométrico confunde a dos personas diferentes indicando que son la misma persona.
(Fuente: CCN)

Tasas de falsos negativos inferiores a 0.005. (Fuente: CCN)

Es decir, sólo el 0,5% de las personas legítimas son rechazadas de forma incorrecta. (Fuente: CCN)

ribas

Única alternativa para la autenticación presencial

Los sistemas biométricos son el único mecanismo automático que permite acreditar la identidad real de una persona en un control de acceso. (Fuente: CCN)

ribas

Contraseña

Algo que el interesado sabe (ENS)

Puede ser robada o cedida a un tercero
por el propio usuario

Tarjeta de acceso

Algo que el interesado tiene (ENS)

Puede ser robada o cedida a un tercero
por el propio usuario

Cara o huella dactilar

Algo que el interesado es (ENS)

Puede ser robada o cedida a un tercero
por el propio usuario

Factor de inherencia

La utilización del factor de inherencia, que es consustancial a la biometría, aporta una garantía de identidad real que no se puede obtener de los factores de posesión o conocimiento, los cuales pueden ser cedidos o sustraídos por otras personas. (Fuente: Guía del CCN).

Presunción de identidad

El uso de **contraseñas y de tarjetas de acceso** genera una presunción de identidad en relación con su titular, pero no acredita la identidad real, ya que la contraseña puede ser cedida a un tercero o robada.

Conclusión

El único mecanismo automático que permite acreditar la identidad real de una persona es el sistema biométrico

(Fuente: CCN)

Gran hermano y datos biométricos

El principal objetivo del Reglamento de IA en relación con los datos biométricos es prevenir su uso conjunto con la IA para el control del ciudadano

ribas

George Orwell en el Reglamento de IA

Muchos preceptos del Reglamento de IA van orientados a prevenir el futuro distópico que Orwell anticipó en su famosa novela “1984”, publicada en 1949.

ribas

El gran hermano te vigila

Gran Hermano (Big Brother) es el líder omnipresente y omnipotente del régimen totalitario que gobierna el mundo ficticio de Oceanía.

Su imagen aparece por todas partes, con el lema:

"Big Brother is watching you"
("El Gran Hermano te vigila").

Su rostro es el símbolo del control absoluto del Estado, que lo vigila todo mediante tecnología y cámaras.

Riesgos distópicos previstos en el RIA

El gran temor del legislador al redactar el RIA se ve claro en los riesgos que intenta prevenir:

1. Identificación biométrica remota en tiempo real en espacios públicos.
2. Categorización biométrica.
3. Inferencia de emociones mediante datos biométricos.
4. Calificación y puntuación de ciudadanos.
5. Creación de bases de datos mediante extracción no selectiva de imágenes faciales de internet o circuitos cerrados de TV.
6. Predicción de delitos.
7. Control fronterizo y migración.

Estos riesgos se asocian a la distopía de un Estado policial y controlador.

Datos biométricos excluidos de la zona de riesgo

El Reglamento de IA excluye los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como confirmar la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso a un local.

El factor diferenciador en este caso es la participación activa del interesado.

Anteproyecto

El Anteproyecto de ley para el buen uso y la gobernanza de la IA también excluye de la lista de sistemas de IA de alto riesgo los sistemas para identificación biométrica remota cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser.

ribas

Eliminar la confusión del ciudadano

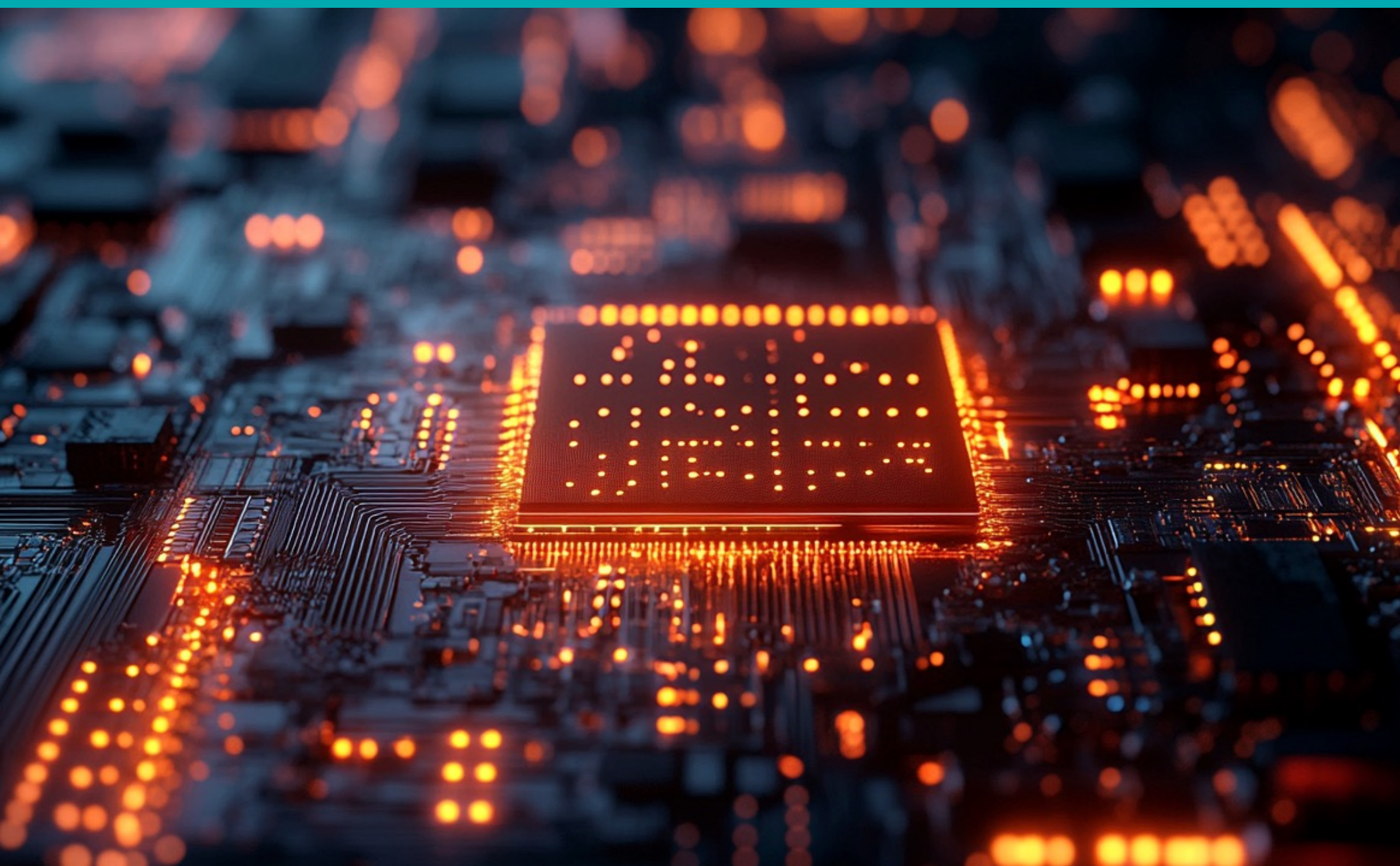
Hasta ahora, el criterio del legislador en el momento de redactar las normas que regulan este tipo de datos se ha basado en el miedo del ciudadano a ser controlado con sus datos biométricos.

Las autoridades de control se han dejado llevar también por una interpretación restrictiva que proscribe el dato biométrico y acrecienta la creencia de que los datos biométricos suponen una gran amenaza para la privacidad.

En paralelo, tanto el poder legislativo como el ejecutivo deberían realizar una función de concienciación que ayude a separar los buenos usos de los malos usos.

Los datos biométricos en la era de la informática cuántica

Alternativas a los sistemas actuales basados en la presunción de identidad



ribas

Amenaza para la seguridad

La informática cuántica supone una amenaza significativa para la seguridad de un sistema informático y de una empresa debido a su potencial para romper los sistemas de cifrado actuales.

ribas

Dificultad actual

Muchos de los criptosistemas utilizados en la autenticación se basan en la dificultad que tienen los ordenadores convencionales para resolver ciertos problemas matemáticos, como la factorización de números enteros y los logaritmos.

ribas

Potencia cuántica

Un ordenador cuántico suficientemente potente podría resolver los problemas matemáticos de manera exponencialmente más rápida que los ordenadores convencionales, lo que significaría que podría descifrar información que actualmente se considera segura, así como suplantar la identidad de un usuario legítimo. Esto pondría en riesgo la confidencialidad de una amplia gama de datos, desde correos electrónicos y registros médicos hasta información financiera y secretos de estado.

ribas

Debilidad de las contraseñas

La informática cuántica podrá romper muchos de los algoritmos de cifrado actuales, como RSA, ECC, gracias a algoritmos como **Shor,** para factorización de claves o **Grover,** para búsqueda en bases de datos.

Esto significa que:

Las **contraseñas tradicionales,** aunque sean largas y complejas, podrían ser descubiertas con relativa facilidad.

La **autenticación basada en conocimiento,** algo que sabes, perderá fiabilidad frente a los avances cuánticos.

NIST

Para contrarrestar la amenaza cuántica, el NIST ha estado trabajando en la estandarización de algoritmos criptográficos resistentes a ataques cuánticos, conocidos como criptografía post-cuántica (PQC).

Los FIPS 203, 204 y 205 son los primeros estándares finalizados que especifican esquemas de establecimiento de claves y firmas digitales diseñados para resistir futuros ataques de ordenadores cuánticos.

Nuevos algoritmos post-cuánticos

Los nuevos algoritmos se basan en diferentes problemas matemáticos que se considera que son difíciles de resolver tanto para los ordenadores convencionales como para los cuánticos.

El NIST está alentando a los administradores de sistemas informáticos a comenzar la transición a estos nuevos estándares lo antes posible.

ribas

Ventajas de los sistemas biométricos

La autenticación biométrica se basa en **algo que eres**: huellas, rostro, voz, iris, patrones venosos, etc. Esto tiene ventajas incluso ante amenazas cuánticas, que:

1. **No se pueden adivinar** con algoritmos cuánticos como sí ocurre con contraseñas o claves privadas.

2. Aunque ciertos rasgos pueden ser replicables (por ejemplo, con deepfakes), los sistemas modernos incorporan técnicas de detección de microexpresiones y otras **pruebas de vida** y comportamiento que tienen que coincidir con las obtenidas directamente del interesado. También están evolucionando rápidamente los **sistemas de IA de detección de deepfakes**, que detectan artefactos, micromovimientos, imperfecciones y otros elementos característicos de los deepfakes, además de la habilidad de la IA para detectar el trabajo realizado por otra IA.

3. Los **datos biométricos no son datos brutos**, sino datos basados en plantillas cifradas e irreversibles.

ribas

Hacia sistemas híbridos e inteligentes

La tendencia parece dirigirse hacia una combinación de biometría con otros elementos como:

1. **Autenticación multifactor:** biometría + hardware token, por ejemplo.

2. **Algoritmos de cifrado post-cuántico** combinados con plantillas biométricas.

3. **Modelos de comportamiento:** patrones de uso del móvil, forma de escribir, ritmo al caminar y otros patrones como capa adicional.

ribas

Cambio cultural

Progresivamente, el uso de datos biométricos para la autenticación del usuario, con su participación activa, dejará de verse por los usuarios y por las autoridades de control como una amenaza basada en un miedo irracional, y pasará a verse como lo que es: una medida de seguridad. La única medida que permite acreditar la identidad real de una persona, según el CCN.

ribas

La autenticación en la era de la inteligencia artificial

Riesgos y ventajas que puede generar el uso de la IA en los procesos de autenticación.

ribas

Ataques de presentación

La inteligencia artificial puede tener un papel importante tanto en la preparación y ejecución de ataques de presentación como en su prevención.

A continuación, veremos algunos ejemplos.

Spoofing mediante imagen o vídeo

Mecánica:

Se muestra al sensor una foto, un vídeo o una pantalla reproduciendo el rostro de la víctima.

Rol de la IA en el ataque:

1. Mejora de la nitidez y el realismo.
2. Corrección de iluminación.
3. Estabilización del parpadeo.
4. Generación de micro-movimientos para simular “pruebas de vida”.

Rol de la IA en la defensa:

1. Detección de artefactos digitales, patrones de pantalla, reflejos no humanos.
2. Detección de modelos de “liveness” basados en micro-expresiones y análisis de profundidad.

Deepfakes de rostro y voz

Mecánica:

Generación sintética de cara o voz para suplantar a alguien.

Rol de la IA en el ataque:

1. Generación de deepfakes hiperrealistas (face-swap, voice cloning).
2. Sincronización labial (“lip-sync”) en tiempo real.

Rol de la IA en la defensa:

1. Detectores de deepfake (análisis de inconsistencias biológicas, parpadeo, compresión).
2. Modelos que verifican concordancia entre audio, vídeo y contexto.

Máscaras 3D y prótesis realistas

Mecánica:

Uso de máscaras de silicona o de impresión 3D para engañar a sistemas de reconocimiento facial.

Rol de la IA en el ataque:

1. Diseño asistido por IA.
2. Aproximación de volúmenes, texturas y tonos de piel.

Rol de la IA en la defensa:

1. Detección de profundidad, termografía, micro-texturas de piel.
2. Modelos que aprenden indicadores de materiales no humanos.

Simulación de huellas dactilares mediante moldes, pegatinas o impresión

Mecánica:

Presentación de moldes de silicona, impresiones 2D/3D sobre el lector..

Rol de la IA en el ataque:

1. Reconstrucción de patrones a partir de imágenes y muestras.
2. Generación de huellas sintéticas creíbles.

Rol de la IA en la defensa:

1. Detección de indicadores de vida (sudor, elasticidad, presión).
2. Análisis de poros y micro-arrugas mediante modelos entrenados.

Iris y retina

Mecánica:

Presentación de lentillas impresas, imágenes del iris, proyecciones..

Rol de la IA en el ataque:

1. Reconstrucción de patrones a partir de imágenes.
2. Generación de patrones de iris sintéticos con alta similitud estadística.

Rol de la IA en la defensa:

1. Medición de indicadores de vida en el iris a través de la contracción pupilar y los reflejos especulares, entre otros.
2. Modelos que distinguen entre impresiones y estructuras orgánicas..

ISO 30107

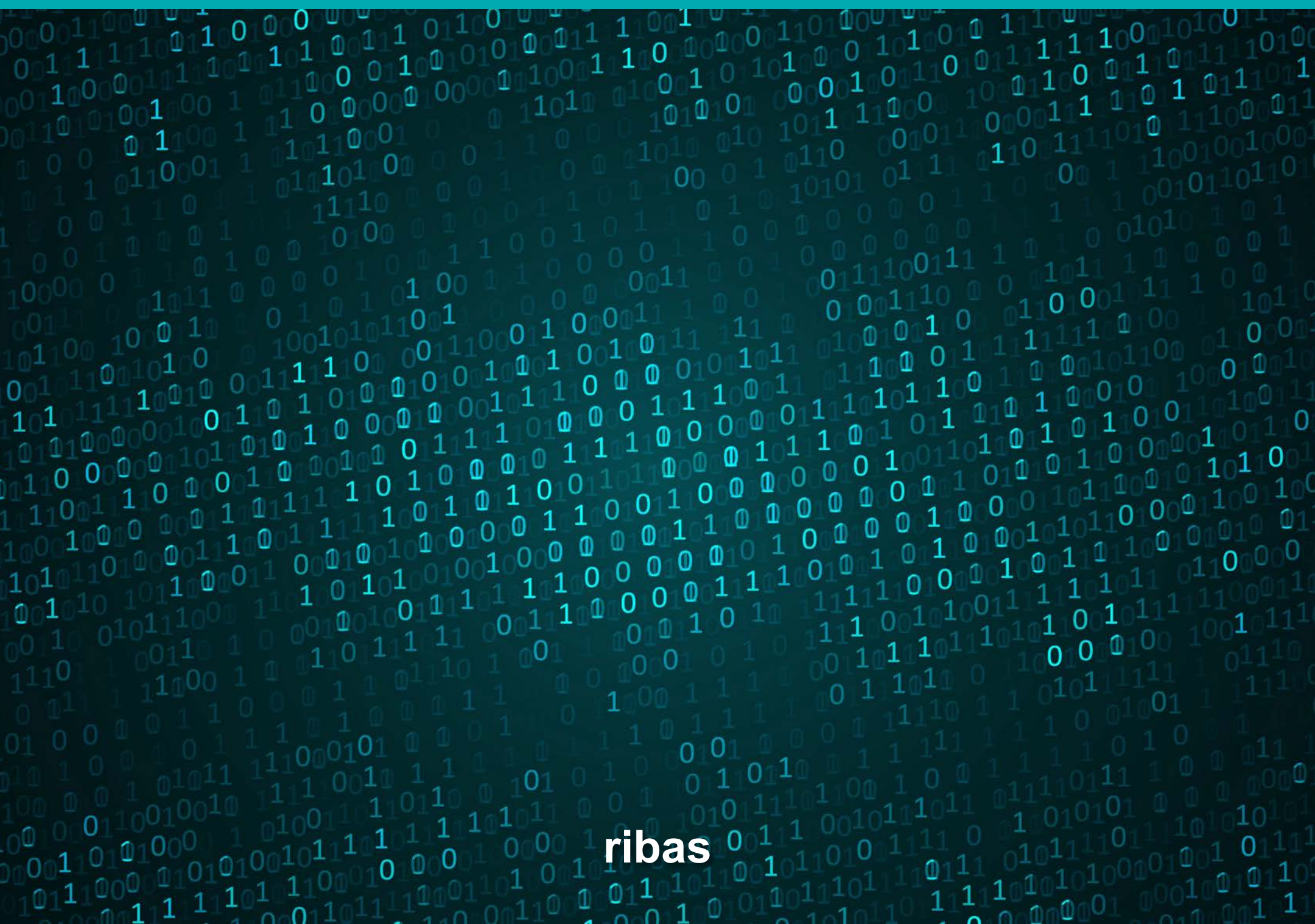
La norma ISO/IEC 30107 es una serie internacional que establece el marco para la **detección de ataques de presentación (PAD)** en sistemas de autenticación biométrica, definiendo cómo probar la "detección de vida" para prevenir el fraude con máscaras, fotos o vídeos, dividiéndose en partes que cubren el marco (Parte 1), los formatos de datos (Parte 2) y las pruebas y reportes de rendimiento (Parte 3). Su objetivo es asegurar que los sistemas biométricos sean fiables frente a intentos de engaño, como el uso de réplicas o imágenes falsas presentadas al sensor.

Esta norma es muy importante para la seguridad en los sistemas biométricos, ya que permite a las organizaciones validar que sus lectores de huellas o reconocimiento facial pueden distinguir a un usuario real de un impostor que utiliza una falsificación a través de un ataque de presentación.

ribas

Combinación de IA e informática cuántica

Predicción de posibles tendencias en la autenticación



Posibles tendencias

En un escenario más próximo de lo que parece, con una IA muy potente y una informática cuántica accesible, las principales tendencias en materia de autenticación podrían evolucionar en las siguientes direcciones:

Factor criptográfico fuerte y rotable

1. Passkeys: FIDO2 almacenadas en hardware seguro (móvil o llave física).
2. Protección mediante algoritmos post-cuánticos.
3. Posibilidad de revocar y regenerar credenciales ante sospecha de compromiso.

Biometría utilizada como sistema local de desbloqueo y no como credencial remota

1. La huella o la cara solo desbloquean la clave en el dispositivo del usuario.
2. El servidor no ve la plantilla biométrica ni la usa como factor primario.
3. Si la IA utilizada por un atacante genera un deepfake del rostro de la víctima, no puede aplicarlo con éxito porque debe ir asociado a la clave privada almacenada en el hardware del usuario.

Factores contextuales y de comportamiento

1. Geolocalización habitual, patrones de uso, dispositivo conocido, horarios.
2. Analítica de riesgo que incrementa los requisitos, por ejemplo, un reto adicional o una revisión manual, en caso de sospecha..

Capa antifraude basada en IA defensiva

1. Detección de deepfakes en videollamadas de alta criticidad, por ejemplo, en transacciones de cuantía, cambios de IBAN, reset de credenciales privilegiadas, etc.
2. Análisis avanzado de patrones de transacciones y comunicaciones para detectar comportamientos atípicos.

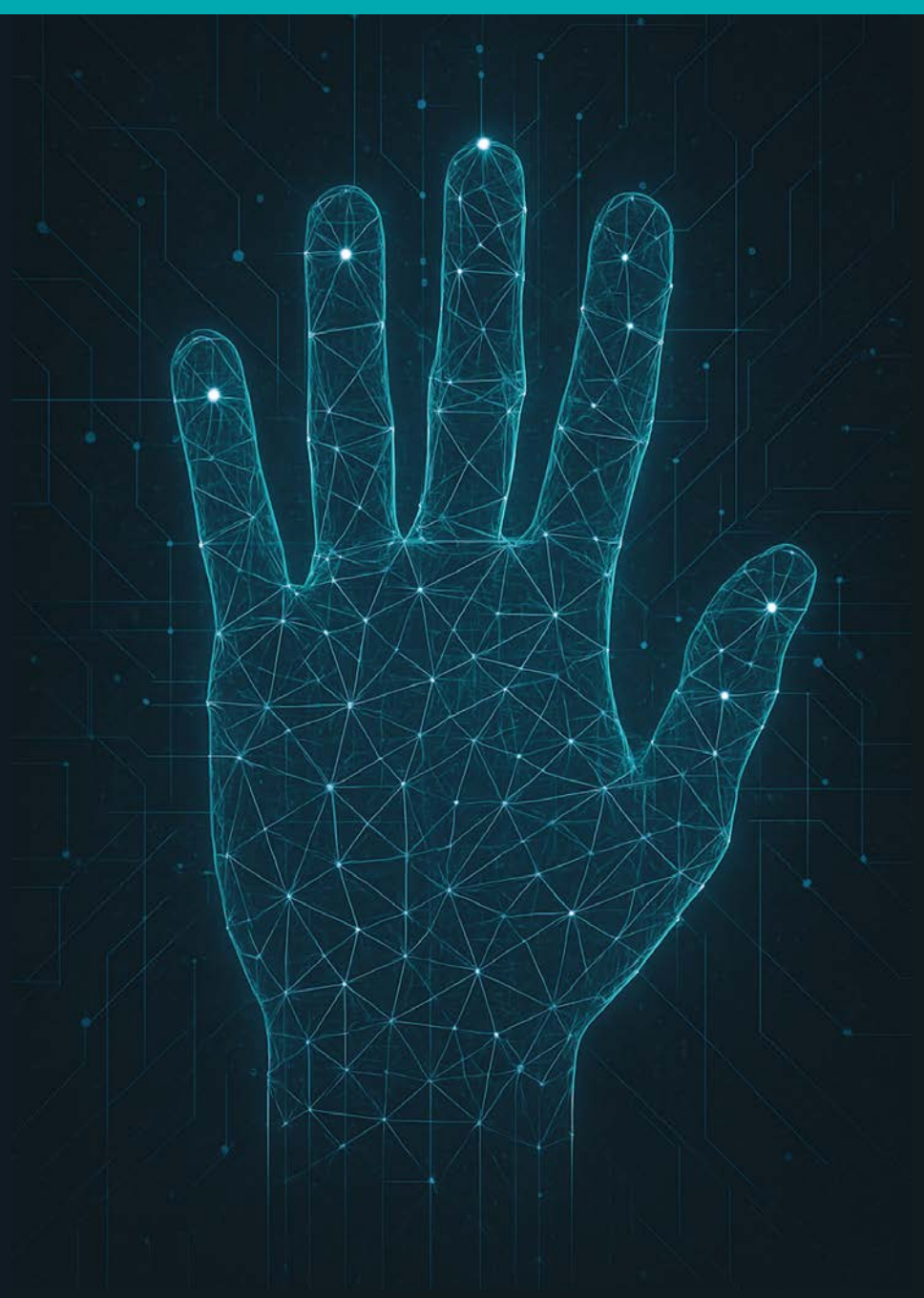
Autenticación local vs. autenticación remota

Tal como puede verse en esta tabla, es muy probable que en el futuro, y a causa de la combinación de la IA con la informática cuántica, se produzca una mayor diferenciación entre la autenticación local y la autenticación remota.

Atributo	Autenticación local	Autenticación remota
Riesgo de uso de la IA en ataque	Bajo	Alto
Posibilidad de uso de la IA en defensa	Alta	Alta
Riesgo de uso de deepfakes	Bajo	Alto
Posibilidad de detección de deepfakes	Alta	Media
Riesgo de suplantación	Bajo	Alto

Lista completa de garantías y medidas

Tabla resumen de las garantías y medidas a aplicar para conseguir un tratamiento de datos biométricos adecuado a los criterios de la AEPD.



ribas

Garantías y medidas a aplicar

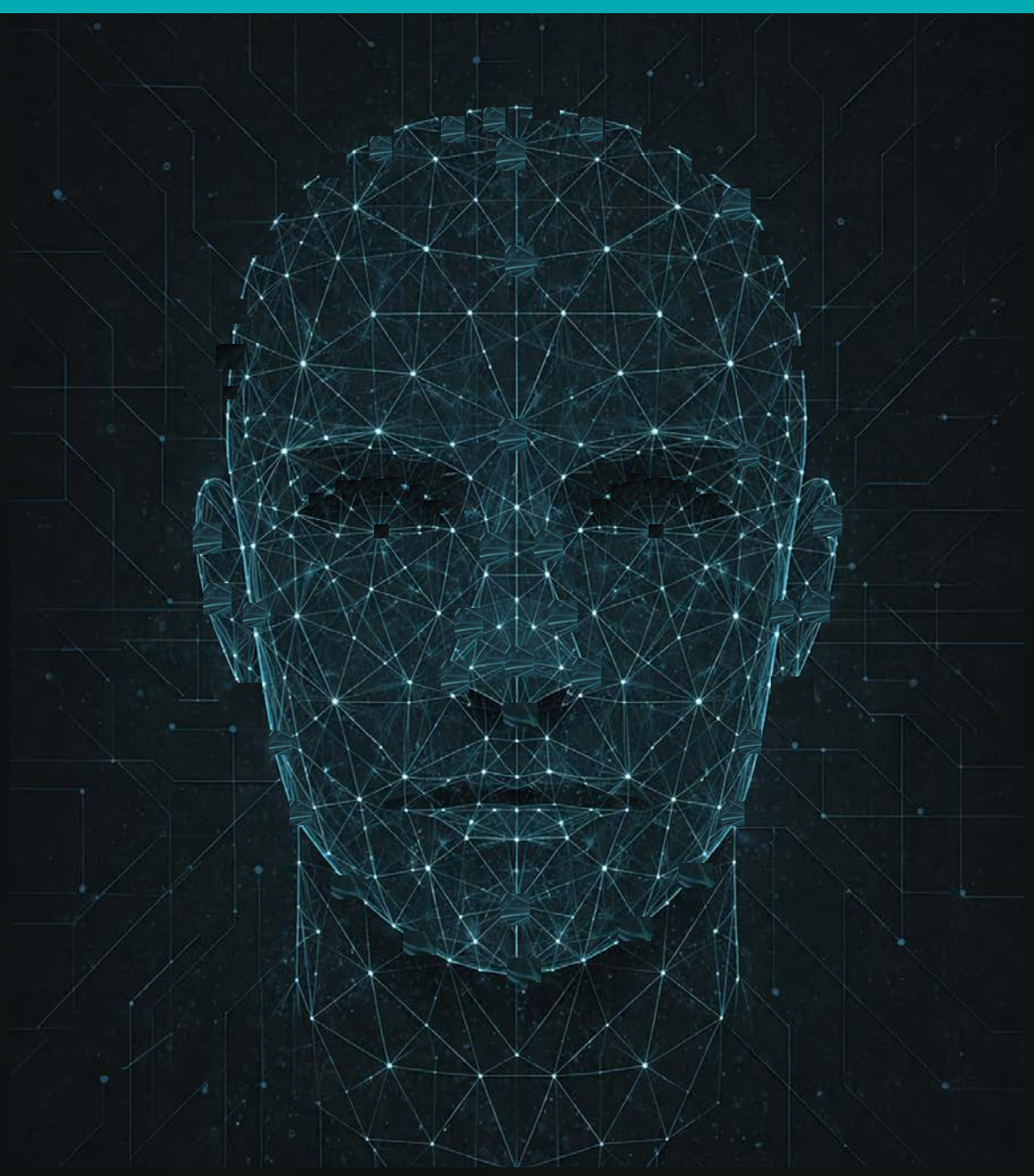
Tabla resumen de las garantías y medidas a aplicar para conseguir un tratamiento de datos biométricos adecuado a los criterios de la AEPD.

#	Garantía o medida
1	Registro biométrico asistido por personal cualificado.
2	Exclusión de procesos de registro desasistidos o delegados en terceros.
3	Datos biométricos bajo el control exclusivo del interesado.
4	Prevención de acceso o tratamiento por terceros.
5	Protección frente al fraude o la suplantación de identidad.
6	Almacenamiento no centralizado de los datos biométricos o con clave del interesado.
7	Generación como tratamiento local, en sistemas aislados, sin conexión a redes
8	Imposibilidad de interoperabilidad con otros sistemas.
9	Revocabilidad de los identificadores.
10	Fecha de caducidad que limite su uso al tiempo estrictamente necesario.
11	Información clara sobre alternativas disponibles, riesgos del tratamiento, derechos del interesado y procedimientos de destrucción de los datos.
12	Conservación de los datos personales no biométricos durante 30 días, con bloqueo posterior.
13	Limitación del almacenamiento de información en los sistemas al tiempo necesario para cada autenticación, sin permitir su transmisión o conservación indebida.
14	Instalación de la infraestructura biométrica en ubicaciones controladas dentro de las propias dependencias de seguridad, en condiciones que garanticen la privacidad y la seguridad técnica.
15	Evaluación de impacto que cumpla los requisitos descritos en este documento: https://lnkd.in/e4CUf4Cy
16	Actualizaciones periódicas de la EIPD al menos cada cuatro años o cuando se produzcan incidentes relevantes o modificaciones sustanciales del tratamiento.
17	Cumplimiento del nivel alto del Esquema Nacional de Seguridad.
18	Auditorías periódicas.

ribas

Conclusiones finales

Tabla de conclusiones finales de los puntos analizados en este informe.



ribas

Conclusiones finales

Las conclusiones de los puntos analizados en este informe son las siguientes:

#	Conclusión
1	El tratamiento de datos biométricos es posible en la actualidad cumpliendo unos requisitos que ahora están más claros y accesibles que en 2024.
2	El control del interesado sobre sus datos biométricos es un requisito importante, que puede cumplirse a través de su almacenamiento en un dispositivo o de forma centralizada con una clave que esté bajo en control exclusivo del interesado.
3	La autenticación 1:1 ofrece menos dificultades a la hora de realizar el análisis de riesgos, valorar la base jurídica, el triple juicio de idoneidad, necesidad y proporcionalidad, la evaluación de impacto y las medidas a aplicar.
4	Es recomendable realizar estos análisis de forma individual para cada finalidad.
5	La evaluación de impacto deberá cumplir los requisitos relacionados en este documento: https://lnkd.in/e4CUf4Cy
6	Un elemento clave del juicio de necesidad es análisis de la viabilidad de las alternativas al control biométrico. El CCN considera este control como el más eficaz.
7	Un elemento clave del juicio de proporcionalidad es el balance riesgo - beneficio.
8	No existen evidencias de un caso de suplantación de identidad ejecutado con éxito mediante la reutilización de plantillas biométricas robadas a un responsable del tratamiento, por lo que todo el riesgo en la creación de deepfakes con IA a partir de los datos biométricos obtenidos de las fotos publicadas en las redes sociales.
9	La detección y neutralización de los deepfakes seguirá un curso parecido al de los antivirus. Cada vez que la IA encuentre la forma de crear un deepfake más potente, la IA defensiva encontrará una forma detectarlo. Todo se reducirá a una lucha entre sistemas de IA que precisará de factores de autenticación adicionales.
10	La seguridad del futuro no depende de un solo factor, sino de la suma de los siguientes: criptografía post-cuántica + hardware seguro + biometría local + IA antifraude.

ribas

Documentos recomendados

Documentos útiles para ampliar la información sobre datos biométricos.

Documento	Enlace
Claves para realizar una evaluación de impacto tras la resolución de AENA	https://lnkd.in/e4CUf4Cy
Datos biométricos: cambios decisivos	https://lnkd.in/dCxFxJma

Datos de contacto

Nombre del despacho	Ribas
Domicilio	Diagonal 640 1C - 08017 Barcelona
Persona de contacto	Xavier Ribas
Correo electrónico	xavier.ribas@ribastic.com
Teléfono fijo	934940748
Teléfono móvil	639108413
LinkedIn	https://www.linkedin.com/in/javierribas/
Web	http://ribas.legal
Blog	http://xribas.com

ribas